Investigating cybercrime

Oerlemans, J.J.

Investigating Cybercrime

Investigating Cybercrime

PROEFSCHRIFT

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 10 januari 2017
klokke 13.45 uur

door

Jan-Jaap Oerlemans

geboren te Barendrecht

in 1985

Promotor:	prof. dr. H.J. van den Herik
Copromotoren:	mr. dr. F.P. Ölçer
	mr. dr. B.W. Schermer

Promotiecommissie:	prof. dr. J.H. Crijns
	prof. dr. P.A.L. Ducheine (Universiteit van Amsterdam)
	prof. dr. G.P. van Duijvenvoorde
	prof. dr. S. van der Hof
	prof. dr. E.J. Koops (Tilburg University)
	prof. dr. H.G. van der Wilt (Universiteit van Amsterdam)

SIKS dissertation series no. 2017-01. The research reported in this thesis has been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems.

Lay-out: AlphaZet prepress, Waddinxveen
Printwerk: Amsterdam University Press

ISBN 978-90-8555-109-6

Preface

Investigating Cybercrime reflects my research journey into the topic of criminal investigations that involve cybercrimes. At the start of my PhD research in 2010, I had the ambition to examine the phenomenon of 'high-tech crime'. I soon found out that criminal substantive law, i.e., the law that deals with criminalising certain behaviours, with regard to cybercrime was already up-to-date in the sense that Dutch law complies with international obligations in that regard. The real challenge with cybercrime lies in criminal procedural law and mutual legal assistance matters, so that became the focus of my research.

Criminal procedural law regulates, amongst other things, privacy-infringing investigative methods. Over time, I learned that much ambiguity exists concerning the regulations for using investigative methods in a digital context. The ambiguity on the applicable regulations hinders evidence-gathering activities and thereby also impedes the combatting cybercrime. Such ambiguity with respect to digital investigative methods is detrimental to the rule of law, since a key element of the rule of law is legal certainty. Individuals involved in criminal investigations should know the *scope* of the investigative powers and the *manner* in which they are applied by law enforcement authorities. Regulations for digital investigative methods are, however, often either non-existent or ambiguous. In part, this can be explained by the quick advancements in information and communication technology (ICT) that have not been taken in consideration in legislation.

In a broader perspective, it is also problematic to apply principles from mutual legal assistance to 'the digital jungle' of the Internet. In that 'jungle', law enforcement authorities of many different States use digital investigative methods across State borders, without physically leaving their own territory. The cross-border unilateral application of digital investigative methods can violate the territorial sovereignty of other States and can affect the rights and freedoms of individuals that live abroad. The cross-border unilateral application of digital investigative methods fundamentally affects the current fabric of international cooperation in criminal matters.

In this PhD thesis, I hope to provide more insight into the workings of cybercrime investigations and to contribute to the creation of a legitimate legal framework that regulates digital investigative methods. The manuscript was closed on 24 October 2016. Any changes in the law that have since occurred could not be included. Let us now start with addressing the fascinating questions that cybercrime and digital investigations provide. I wish you pleasant reading.

Jan-Jaap Oerlemans
October 2016, Leiden

Table of Contents

List of abbreviations

CFR	–	Charter of Fundamental Rights of the European Union
CJEU	–	Court of Justice of the European Union
DCCP	–	Dutch Code of Criminal Procedure
DDoS	–	Distributed Denial of Service
DEA	–	Drug Enforcement Agency
DoJ	–	Department of Justice
ECHR	–	European Convention on Human Rights
ECPA	–	Electronic Communications Privacy Act
ECtHR	–	European Court of Human Rights
ENISA	–	European Union Agency for Network and Information Security
EU	–	European Union
FBI	–	Federal Bureau of Investigation
GPS	–	Global Positioning System
HR	–	Hoge Raad (Eng: Supreme Court)
I2P	–	Invisible Internet Project
ICE	–	Immigration and Customs Enforcement
ICT	–	Information and Communications Technology
IP	–	Internet Protocol
IRC	–	Internet Relay Chat
IRT	–	Interregionaal Recherche Team (Eng: Interregional Detective Team)
ITU	–	International Telecommunications Union
NIST	–	National Institute of Standards and Technology
OSINT	–	Open Source Intelligence
Par.	–	Paragraph
PGP	–	Pretty Good Privacy
PS	–	Problem Statement
Rb.	–	Rechtbank (Eng: Court)
RQ	–	Research Question
SaaS	–	Software as a Service
SCA	–	Stored Communications Act
Stb.	–	Staatsblad (Eng: Statute book)
Stcrt.	–	Staatscourant (Eng: State Gazette)
TFEU	–	Treaty on the Functioning of the European Union
Tor	–	The Onion Router
Trb.	–	Tractatenblad (Eng: Treaty Series)
UNODC	–	United Nations Office on Drugs and Crime
U.S.	–	United States
U.S.C.	–	United States Code
U.S. CFR	–	United States Code of Federal Regulations
VPN	–	Virtual Private Network

1 Updating the legal framework

Investigating cybercrime is challenging. Criminals can take advantage of computers and the Internet to commit cybercrimes relatively anonymously and across State borders. They can also reach many computer users without much extra effort by automating their crimes. In cybercrime investigations, there are typically few leads available that law enforcement officials can follow in order to gather evidence and prosecute. Furthermore, computer users can take measures to conceal their identity and hide evidence. Law enforcement officials must overcome these challenges in order to gather evidence successfully. At the same time, law enforcement officials can also take advantage of computers and the Internet in their evidence-gathering activities. For example, they can interact with other computer users via the Internet under the disguise of a 'nickname' (a pseudonym) or hack into computers to gather data, and thereby obtain information that is relevant in a criminal investigation. In doing so, law enforcement officials can make use of the same anonymity and (global) scale that the Internet provides to criminals.

From a legal point of view, the first question that should be asked is whether the investigative methods that are used in an online context are adequately regulated in the domestic legal framework investigating law enforcement officials operate in. The legal frameworks for investigative methods are often designed to accommodate the application of investigative methods in a physical, territorial world that is confined by State borders. In contrast, evidence in cybercrime investigations is often gathered from computers in a borderless networked environment. The domestic legal framework of the investigating law enforcement officials may or may not indicate with sufficient clarity which regulations are applicable. In addition, when the digital application of investigative methods interferes with fundamental rights in a significantly different manner than the application of equivalent investigative methods in the physical world, it may be necessary to change the law accordingly, to accommodate differences.

The second question that should be addressed is whether the application of digital investigative methods has extraterritorial effects. The principle of the territorial restriction of enforcement jurisdiction governs the application of investigative methods, restricting the power to apply investigative methods to the territorial borders of a State. This principle protects the territorial sovereignty of States and ultimately prevents conflicts between States that may be caused by law enforcement officials who cross State borders without the basis of a (mutual legal assistance) treaty or permission from the affected State. As a corollary of this principle, citizens of States are protected from interferences with their fundamental rights by foreign law enforcement

officials who apply their own laws concerning investigative methods. The Internet however, easily allows law enforcement officials to gather evidence unilaterally, i.e., without permission from the affected State or a treaty basis that authorises the evidence-gathering activity, through the use of digital investigative methods. As such, tension may arise with the principle of the territorial restriction of enforcement jurisdiction. The extent to which the cross-border unilateral application of digital investigative methods is acceptable should be examined.

Aim and approach of the study

This study aims to answer the question of how the Dutch legislator can adequately regulate digital investigative methods in Dutch criminal procedural law. In this context, 'adequately regulating digital investigative methods' means that the regulation of investigative methods (1) provides the necessary instruments for law enforcement officials to gather evidence in cybercrime investigations and (2) provides the individuals involved with a minimum of protection, as required by relevant human rights treaties. In relation to the latter, the focus is on article 8 of the European Convention on Human Rights (hereinafter: ECHR), which protects the right to privacy. The approach taken in this regard is outlined below.

First, the digital investigative methods to be examined in this study are identified by explaining how evidence is obtained in cybercrime investigations. The challenges of anonymity and encryption in cybercrime investigations are also discussed, showing how up-to-date investigative methods should be used to overcome these challenges. The analysis of digital investigative methods and the challenges of anonymity and encryption takes place in chapter 2. The challenge of jurisdiction in these investigations is also introduced in chapter 2, accompanied by an explanation of how digital investigative methods can be applied across State borders and unilaterally in order to overcome this challenge.

Second, the adequacy of the pertinent regulations is tested by analysing the extent to which Dutch criminal procedural law, given the special features of digital investigative methods, requires updates to accommodate the investigative methods. In order to determine the adequacy of the Dutch legal framework in relation to human rights, Dutch regulations are tested with regard to the normative requirements that can be derived from art. 8 ECHR. These normative requirements are determined in chapter 3. In chapter 4, the desirable quality of the law that is derived from art. 8 ECHR is determined for the identified digital investigative methods. Chapters 5 to 8 then examine whether the Dutch legal framework adequately accommodates these investigative methods.

Third, the legitimacy of the cross-border unilateral application of digital investigative methods is analysed by examining issues attached to such practices. More particularly, chapter 9 examines how the cross-border uni-

lateral application of these investigative methods may interfere with State sovereignty and the legal certainty of the individuals involved.[1]

Structure of this chapter
This chapter is structured as follows. Section 1.1 provides a further characterisation of this study. Section 1.2 presents the problem statement and five research questions. In section 1.3, the restrictions of the study are specified. Section 1.4 explains the research methodologies used to answer the research questions. Finally, section 1.5 presents an overview of the structure of the study.

1.1 Characterisation of the study

The emphasis of this study, *Investigating Cybercrime*, is on the relationship between technology and the legitimacy of a criminal justice system. To ensure the legitimacy of such a system, the scope and conditions for the application of digital investigative methods must be clear. All actors involved in the criminal justice system – i.e., law enforcement officials, the individuals involved in a criminal investigation, public prosecutors, lawyers, and judges – must have clarity about both the legal basis for investigative methods and the conditions under which law enforcement officials can apply them. An accessible and foreseeable legal framework for investigative methods helps prevent arbitrary application of power by governmental authorities; it is therefore essential for protecting the rule of law. The legal framework must also comply with overarching legal norms, such as those contained in the ECHR, to provide citizens with at least a minimum level of protection against arbitrary application of governmental power. At the same time, in order to be able to correctly identify normative requirements, understanding of the technology of digital investigative methods is required. Thus, to determine whether a legal framework complies with overarching legal norms such as those contained in art. 8 ECHR, it is necessary to analyse how digital investigative methods are applied and affect fundamental rights. If they affect human rights in a different manner than non-digital 'equivalent' methods, it is examined how such differences should be accommodated in legal frameworks.

1 The term legal certainty is used to refer to the requirements of art. 8 ECHR, against which Dutch law will be tested. However, in the context of the subject matter of chapter 9, the term legal certainty should also be understood more broadly in terms of rule of law requirements. The content of legal certainty as meant in this study, will become evident in chapter 9.

The emphasis chosen has implications for the nature of this study, which may be characterised as a hybrid study involving interfaces between various fields. On the one hand, these fields are legal, with the study examining human rights law, criminal procedural law, and information and communication technology law (ICT law).[2] On the other hand, the study also draws on insights from computer science.

The hybrid characterisation is important for two reasons, both of which have to do with the scope. First, although it is impossible to evaluate the legitimacy of regulations without understanding the technology involved, the examination of that technology in this study can go no further than the basics. Second, given the broadness of the legal subject matter, consisting of several different legal fields, it is likewise not possible to exhaustively analyse all relevant aspects of the various legal fields involved. This study will thus not integrally examine neither the technology nor the law involved, but should be seen as an explorative overview, with the overall aim to understand the misalignments that can occur in the practice of applying digital investigative methods and the theory in the applicable legal frameworks.

Format of the study

In this regard it is important to present the format of this study. As stated earlier, the normative requirements for the regulation of digital investigative methods are derived from art. 8 ECHR. The legal framework that is tested against these normative requirements is Dutch law, which serves as an appropriate object of study for three reasons.

The first reason is that digital investigative methods are already applied in Dutch practice.[3] Unlike criminal substantive law (which is regularly updated to accommodate cybercrimes), very little has been done to rethink the criminal procedural frameworks to accommodate digital investigative

2 This study will also incorporate pertinent international law instruments.

3 See, e.g., Landelijk Parket, 'Dutch National Crime Squad announces takedown of dangerous botnet', 25 October 2010. Available at: https://www.om.nl/actueel/nieuwsberichten/@28332/dutch-national-crime/, Landelijk Parket, 'Onderzoek Holitna: meer dan 500 kinderpornozaken', 30 May 2012. Available at: https://www.om.nl/onderwerpen/kinderporno/@30624/onderzoek-holitna/, Landelijk Parket, 'Undercover onderzoek naar illegale marktplaatsen op Internet', 14 February 2014. Available at: https://www.om.nl/@32626/undercover-onderzoek/, Landelijk Parket, 'Wereldwijde actie politie en justitie tegen hackers'. Available at: https://www.om.nl/vaste-onderdelen/zoeken/@85963/wereldwijde-actie, and Landelijke Parket, 'Anonieme, illegale marktplaatsen op internet aangepakt', 24 November 2015. Available at: https://www.om.nl/@91879/anonieme-illegale/ (last visited on 30 May 2016).

methods in the Netherlands.[4] This means that in practice, when digital investigative methods are currently applied, they are based on regulations that have been designed for offline applications. In the 1990s, the Dutch legislature already posited conceptually that the 'offline laws' are also applicable 'online'.[5] However, a conceptual statement alone does not provide clarity about the scope and the manner in which digital investigative methods are applied. Earlier research indicates that it is unclear for law enforcement officials which legal basis applies to digital investigative methods (cf. Stol, Leukfeldt & Domenie 2013, p. 79).[6] As such, Dutch law provides a useful scenario for determining whether misalignment between human rights law, domestic law, and technology exists.

The second reason is that the Netherlands is a member of the Council of Europe and as such a signatory State to the ECHR. This means that Dutch law must comply with art. 8 ECHR, which is the overarching legal framework that is tested in this study.[7] As a result, this study is also relevant for other Council of Europe members. The analysis of Dutch law in terms of compliance with art. 8 ECHR will thus provide a basis for evaluation of compliance in that sense for other Council of Europe jurisdictions.

The third reason is that the Netherlands has a civil law system with a strong commitment to the principle of legality. This means that legal certainty standards are heightened in the Netherlands, as is common in continental legal systems. In the Netherlands, the pre-trial investigative stage is particularly dominated by the 'criminal procedural legality principle' (see Kooij-

4 The implementation of the Treaty of Lanzarote of 2007 (*Trb*. 2010, 156) and the EU Directive 2013/40/EU on 'attacks against information systems' (L218/8) of 14 August 2013 (*Stb.* 2015, no. 165) last updated Dutch criminal substantive law with regard to cybercrime. Dutch criminal procedural law has not been amended to accommodate digital investigative methods between 2006 and 2015. In 2014, major revisions of Dutch criminal procedural law were proposed and published by the Dutch Ministry of Security and Justice. The ambitious project of 'Modernising Dutch criminal procedural law' aims to make the law 'technologically neutral and future-proof'. Yet, the proposals in the project only seek to amend regulations for computer searches as an investigative method. See Ölçer 2015 for an overview of the concept bill with regard to special investigative powers. In addition, in 2015, a bill for a third Computer Crime Act incorporated a proposal to accommodate hacking as an investigative method in Dutch criminal procedural law. No other digital investigative methods are regulated by these proposals.

5 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1997/98, 25 880, no. 1, p. 1.

6 Also note that, in a letter to the Dutch parliament in 2009, the Dutch minister of Security and Justice stated: "*There is a great need among law enforcement officials for explanation about the applicable legislation and application of (special) investigative powers on the Internet*" (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2008/09, 28 684, no. 232, p. 2-3).

7 For the regulation of criminal procedural investigative methods, emphasis is often placed on art. 8 ECHR in the Netherlands. See, e.g., *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 9-13, *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 4-6 and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 56-59.

mans & Mevis 2013, p. 3). Art. 1 of the Dutch Code of Criminal Procedure (hereinafter DCCP) articulates this principle as follows: *"criminal procedure is only carried out in the manner provided by law"*.[8] Essentially, in the context of criminal investigations, this principle dictates that the evidence-gathering activities of law enforcement officials must be regulated in the DCCP.[9] The promotion of legal certainty is the central objective of the criminal procedural legality principle (cf. Corstens & Borgers 2014, p. 19).[10] The criminal procedural legality principle brings with it that for intrusive investigative methods, Dutch law requires a legal basis in clear and detailed (statutory) regulations. As such, within other Council of Europe member state jurisdictions, the Netherlands provides a good model for study. The reason is that ECHR standards are 'minimum' standards, which are applicable in 47 different jurisdictions. Differences between the legal systems of member states can bring with them that variation exists in the manner in which ECHR standards are applied domestically. As long as domestic application does not fall short of the minimum standards of the ECHR, the treaty allows for divergence. In terms of the principle of legality in criminal procedural law, divergence may exist in terms of the manner in which criminal procedure is regulated. So, in some Council of Europe member states' legal systems, domestic requirements for legal bases for investigative methods may not be as strict as those in others. With its heightened domestic requirements in terms of the principle of legality, Dutch law will thus require analysis of pertinent ECHR normative requirements in 'full force'.

The 'IRT affair'

It is relevant in this respect to mention earlier experiences in the Netherlands with regards to the regulation of new investigative methods. In the beginning of the 1990s, Dutch police forces cooperated in 'Interregional Detective Teams' (in Dutch, *Interregionale Recherche Teams*, or IRT) to combat serious organised crime. Inspired by U.S. law enforcement officials who used deep-cover operations to investigate (in particular) drug-related crimes, Dutch law enforcement officials made extensive use of paid informants and under-

8 Here, 'law' means statutory laws established by acts of the House of Representatives and reviewed by the Dutch Senate. Thus, in the Netherlands, the legislature decides which criminal procedure regulations apply. The underlying idea is that the creation of criminal procedural law cannot be left to judges, not even implicitly, as a result of ambiguous procedures for investigative methods that leave too much room for interpretation by judges (see Corstens & Borgers 2014, p. 19).

9 Procedures with regard to administrative or technical aspects of investigative methods can be regulated outside criminal procedural law. See also the letter regarding the contours of the project, 'Modernising Criminal Procedural Law', of 30 September 2015, p. 10-11. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (last visited on 23 March 2016).

10 For a more extensive analysis regarding the backgrounds of the legality principle in criminal procedural law, see Simmelink 1987 and Groenhuijsen & Knigge 2004, p. 11-16.

cover agents to acquire information about criminal organisations.[11] Selected law enforcement officials and a few public prosecutors authorised the (un) controlled delivery of drugs transports in order to build up credibility and maintain the cover of undercover agents. Therewith, drugs were allowed to reach the market.[12] The use of paid informants and authorised drug transports was poorly reported by the law enforcement officials and in part kept undisclosed during ensuing trials.[13]

Ultimately, the use of new investigative methods became public and led to unrest within the Dutch society. The event was dubbed the 'IRT affair', named after the teams that applied the controversial investigative methods. An inquiry was subsequently conducted by the parliamentary inquiry commission Van Traa, which delivered an extensive report on the use of special investigative methods by Dutch law enforcement officials and made recommendations for new regulations. In part, these recommendations eventually led to the Special Investigative Powers Act, which was adopted in 1999.[14] The act reinforced the rule that investigative methods that interfere with the rights and freedoms of individuals in more than a minor way or threaten the integrity of a criminal investigation must be regulated in detail in the DCCP.[15]

Lesson learned?

The history of the legislative reforms regarding undercover investigative methods should evoke the continued consciousness Dutch legislature. In particular, new investigative methods may again require amendments to legislation. The explanatory memorandum of the Special Investigative Powers Act explicitly notes that the Dutch legislature is charged with the task of amending or creating new legislation when:

---

11 See for an extensive analysis, see Nadelmann 1993, Nadelmann 1995, in: Fijnaut & Marx 1995, Fijnaut and Marx 1995 in: Fijnaut & Marx 1995.

12 See for extensive description about the investigative methods used: *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1995/96, 24 072, no. 10-11 (Van Traa Report), p. 72-164.

13 In addition, the majority of the public prosecutors and the minister of justice were not sufficiently informed about these interregional detective teams' investigative methods. See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1995/96, 24 072, no. 11 (Van Traa Report), p. 427-428.

14 *Stb.* 1999, 245, 27 May 1999 (entered into force on the 1 February 2000).

15 This standard was first set in the landmark case of Zwolsman in 1995, in which the Dutch Supreme Court decided that searching the trash bags of citizens was not a privacy-infringing investigative method to the extent that it required detailed regulations in the Dutch Criminal Procedural Code (HR 19 December 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996, 249 m nt. Schalken). This standard was later affirmed with regard to other investigative methods by the Dutch legislature in *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum to the Special Investigative Powers Act), p. 110 and 115 and the Dutch Supreme Court (see, e.g., HR 20 January 2009, ECLI:NL:HR:2009:BF5603, *NJ* 2009, 225, m.nt. Borgers, HR 13 November 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013, 413, m.nt. Borgers and and HR 1 July 2014, ECLI:NL:HR:2014:1562, *NJ* 2015/115, m.nt. P.H.P.H.M.C. van Kempen).

"developments in crime – that often find their origin in technological developments – require the application of new investigative methods that interfere with the right to privacy of involved citizens in more than a minor way".[16]

With the development of digital investigative methods, the task of critically reviewing the adequacy of existing frameworks and, if necessary, adopting new legislation has become one of utmost importance.[17] These digital investigative methods have as of yet not been clearly defined by law. The digital investigative methods are applied in a covert manner, which makes them particularly sensitive in terms of art. 8 ECHR and similar to the investigative methods which were eventually regulated in the Special Investigative Powers Act in 1999. The implications of their technological functions must be examined to understand their relationship with the law.

1.2 Problem statement and research questions

The Dutch legal framework must provide law enforcement officials with the instruments they need to obtain evidence when investigating crimes in today's networked world. At the same time, it must adequately protect citizens' fundamental rights and freedoms. The problem statement (PS) is formulated as follows.

PS: *To what extent does Dutch criminal procedural law adequately regulate the investigative methods used in (cross-border unilateral) cybercrime investigations?*

Five research questions are formulated to answer the problem statement.

The first research question aims to identify the investigative methods that are commonly used in cybercrime investigations. It is formulated as follows.

RQ 1: *Which investigative methods are commonly used in cybercrime investigations?*

16 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 12 (all texts from parliamentary proceedings are translated by the author).

17 See also the Council of Europe Recommendation Rec(2005)10 to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism, adopted by the Committee of Ministers on 20 April 2005: *"Considering that special investigation techniques are numerous, varied and constantly evolving and their common characteristics are their cover nature and the fact that their application could interfere with fundamental rights and freedoms"* (also adopted by the Draft Recommendation on "special investigation techniques" in relation to serious crimes including acts of terrorism, consolidated by the SIT Drafting group at its second meeting (Rome, 13-14 June 2016)).

In order to identify the relevant investigative methods, an analysis is conducted to ascertain (1) which digital leads law enforcement officials typically follow, (2) which investigative methods law enforcement officials subsequently utilise to gather evidence based on these digital leads, and (3) which investigative methods are used to overcome the challenges of anonymity and encryption in cybercrime investigations.

The second research question aims to determine the requirements that art. 8 ECHR imposes on the domestic legal frameworks of contracting States to regulate investigative methods *generally*. It is important to note that art. 8 ECHR and the accompanying case law of the European Court of Human Rights (hereinafter: ECtHR) with regard to this provision are not specifically developed for application in a digital context. Although in recent case law, the ECtHR has started to develop its thinking about the relationship between the treaty and the digital world, case law in this regard is sparse. Chapter 3 discusses requirements as they apply generally. The manner in which this general framework should apply to the digital context is discussed in the ensuing chapters (particularly chapter 4). The second research question is formulated as follows.

RQ 2: *Which normative requirements can be derived from art. 8 ECHR for the regulation of investigative methods?*

The third research question aims to determine what requirements exist for the regulation of the identified digital investigative methods. Depending on the gravity of the privacy interference, the ECtHR may require detailed regulations and specific procedural safeguards. Contracting States to the ECHR, including the Netherlands, must implement these requirements in their domestic legal frameworks. The requirements for digital investigative methods are determined by positioning the identified digital investigative methods in the existing general framework in art. 8 ECHR. This will be done by analysing the gravity of the privacy interferences involved in the application of the digital investigative methods (in light of their technological functions) and on that basis, determining what type of regulations is desired. The third research question is formulated as follows.

RQ 3: *Which quality of law is desirable for the identified digital investigative methods?*

The fourth research question aims to determine how the Dutch criminal procedural law that regulates the identified digital investigative methods can be improved by taking the identified normative requirements of art. 8 ECHR into consideration. The Dutch legal framework is considered adequate when the normative requirements from art. 8 ECHR are met. The fourth research question is formulated as follows.

RQ 4: *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate the identified investigative methods?*

The issue here is whether the basis that is currently used in practice for applying digital investigative methods is adequate, given the technical and legal implications of these methods. The research field for RQ 4, i.e., the application of digital investigative methods, is rather wide. To answer the research question, the following four investigative methods are examined (each in a separate chapter). [In passing, it is noted that here the answer to RQ 1 is anticipated upon.]

(RQ 4a) Gathering publicly available online information (chapter 5)
(RQ 4b) Issuing data production orders to online service providers (chapter 6)
(RQ 4c) Applying online undercover investigative methods (chapter 7)
(RQ 4d) Performing hacking as an investigative method (chapter 8)

The fifth research question is related to the international dimension of cybercrime investigations, which becomes apparent in two situations. First, when the suspect involved in a criminal investigation resides on foreign territory. Second, when evidence (often stored on computers) is located on foreign territory. In these situations, the law enforcement officials who investigate cybercrime commonly have to gather evidence on foreign territory.

Mutual legal assistance is the formal method for obtaining evidence that is located abroad. However, the Internet allows law enforcement officials to utilise certain investigative methods across borders, without the need to physically enter another State. Nonetheless, this unilateral application of investigative methods produces extraterritorial effects on foreign territory and may be questioned on the basis of the territorial limitation of enforcement power, as an established principle in international law. The fifth research question is formulated as follows.

RQ 5: *To what extent is it desirable and legitimate that the identified investigative methods are applied unilaterally across State borders?*

The fifth research question is answered by taking into account (1) the possible infringement of the effected State's territorial sovereignty and (2) the legal certainty of the individuals involved. States have different perspectives on the extent to which investigative methods can be applied across State borders. To illustrate these different perspectives and the implications thereof, a legal comparison between the Netherlands and the United States is conducted.[18]

18 See subsection 1.4.2 for the research methodology of the conducted comparative legal research.

1.3 Restrictions of the research

This research is restricted by focusing on evidence-gathering activities that are conducted by law enforcement officials in cybercrime investigations. The evidence-gathering activities are examined in their relation with the right to privacy as articulated in art. 8 ECHR. The focus gives rise to three restrictions, which are further discussed below.

1.3.1 Restriction to cybercrime investigations

This study focuses on digital investigative methods that are used in criminal investigations that involve cybercrime. Cybercrime is defined as *"criminal acts committed using electronic communication networks and information systems or against such networks and systems"*.[19] Cybercrime is often distinguished as:

(1) target cybercrimes: crimes in which the computer is the target of the offense.
(2) tool cybercrimes: crimes in which the computer is used to facilitate a traditional crime.
(3) crimes in which the use of the computer is an incidental aspect of the commission of the crime, but significant to law enforcement because computers contain traces of evidence of a crime.[20]

Criminal investigations with regard to crimes in which digital evidence only plays a significant role are not considered as cybercrime investigations in this study. Digital evidence is nowadays involved in almost all criminal investigations (cf. Brenner 2010, p. 37). Cybercrime investigations that involve target cybercrimes and tool cybercrimes are more interesting for this research, since investigating these crimes often requires law enforcement officials to follow specific digital leads across State borders, which creates an interesting dynamic to the investigation of these crimes. In addition, the challenges that are often present in these cybercrime investigations require law enforcement officials to use novel digital investigative methods that are of interest to this study.[21]

19 See Communication of 22 May 2007 from the European Commission, 'Towards a General Policy on the Fight against Cybercrime', COM(2007)267 final, p. 2.

20 See Charney 1994, p. 489. Cf. Brenner 2010, p. 39-47. The categorisation closely resembles the categorisation originally made by Parker back in 1976 (Parker 1976, p. 17-22).

21 The search of a place and subsequent seizure of computers and (internet) wiretapping are also investigative methods that are commonly used in cybercrime investigations. However, these investigative methods have a solid basis in Dutch criminal procedural law and are not considered as novel digital investigative methods that require specific analysis.

1.3.2 Restriction to evidence-gathering activities by law enforcement officials

The focus is on the evidence-gathering activities in criminal investigations with regard to cybercrime that are carried out by law enforcement officials. Many of the investigative methods that law enforcement officials use to gather evidence are regulated in the DCCP. The regulation of investigative methods in other legal frameworks are not examined.

The restriction to evidence-gathering activities by law enforcement officials also means that investigative activities in the context of cyberterrorism, cyberespionage, and cyberwar are not examined. Other governmental authorities than law enforcement authorities investigative cyberespionage, as well as 'cyberattacks' that rise to the level of terrorism or war. Those activities are regulated by different legal frameworks. This study only focuses on criminal procedural law. More particularly, only the regulations of investigative methods that can be used by law enforcement officials in 'regular criminal investigations', which start when a reasonable suspicion of a crime exists, are analysed. These investigative methods may be regulated as 'investigative powers' or 'special investigative powers' in Titles IV and IVA of the DCCP. The investigative powers and special investigative powers that can be used in criminal investigations when (1) a reasonable suspicion is present that crimes are being planned or committed in an organised crime context (Title V) and (2) indications are available that terrorist crimes are being planned (Title VB), are not examined in this study. Special investigative powers that can be applied with the aid of civilians (regulated in Title VA and VC) are also excluded from this study. Finally, the regulations for the use of datamining techniques to analyse data in 'explorative investigations' (in Dutch: verkennend onderzoek) in art. 126gg DCCP is not examined.[22]

Governments can also take other measures to deal with the challenges that are arise in cybercrime investigations, such as a decryption order to deal

22 See with regard to use of datamining techniques by law enforcement authorities, e.g., Sietsma 2006 and Brinkhoff 2016. Digital investigations can certainly be a part of investigations under Title V and VB, and differences in the distinct bases for application may be pertinent to the assessment of the adequacy of the specific regulations in different titles. However, given the nature of this study as a non-exhaustive exploration of the relationship between digital investigative methods and the law, the focus will be on the 'standard' application of the methods on the basis of a 'classical' reasonable suspicion of guilt in the sense of art. 27 DCCP. It may be added here that as part of the current modernisation project of the DCCP, the Dutch Ministry of Security and Justice has proposed amendments to redesign the structure of special investigative powers in Dutch criminal procedural law so that the special investigative powers are not regulated three times, but once in the DCCP. The three distinct bases for application will remain however and be regulated in the general provisions of the DCCP. See the discussion document regarding the general provisions for pre-trial investigations (6 June 2014), p. 27-29. Available at: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/herziening-van-het-wetboek-van-strafvordering (last visited 15 November 2015).

with the challenges of encryption.[23] The focus on evidence-gathering activities also brings with that these measures are not examined.

This author is aware that, in practice, policing is not performed by law enforcement officials alone.[24] For instance, private IT security firms, security departments from companies, and online service providers also fight cybercrime. Tensions may arise regarding an individual's right to privacy when these individuals are under investigation by a private organisation. However, criminal procedural law consists of a legal framework that only regulates investigative methods that are used by law enforcement officials.[25] Questions concerning the use of investigative methods by private parties in an online context thus fall outside the scope of this study's problem statement.

1.3.3 Restriction to art. 8 ECHR

This study investigates requirements based on art. 8 ECHR for regulating digital investigative methods in the domestic legal frameworks of States. However, when regulating investigative methods within a domestic legal framework, other fundamental rights – such as the right to a fair trial as specified in art. 6 ECHR – are also important (cf. Ölçer 2008, p. 527-530 and Hirsch Ballin 2012, p. 42-62). Accompanying requirements to ensure a legitimate criminal justice system based on art. 6 ECHR are thus not examined. These requirements include respecting rights such as the privilege against self-incrimination, the prohibition of entrapment, and notifying individuals involved in criminal investigations of the use of investigative methods. The mechanisms that ensure the disclosure of information in the course of crimi-

23 Current (October 2016) debates about measures (1) that require companies to hand over a 'golden key' or 'backdoor' to law enforcement authorities to enable law enforcement officials to acquire decrypted data and (2) enable law enforcement authorities to issue a decryption order to suspects in order to force them to hand over an encryption key to law enforcement authorities under the threat of a prison sentence are not dealt with in this study, since these measures do not concern investigative methods. See, e.g., Bruce Schneier, 'iPhone Encryption and the Return of the Crypto Wars', *Schneier on Security* (blog), 6 October 2014. Available at: https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html and Matt Burgess, 'Tim Cook: Apple won't weaken encryption to meet FBI demands', *Wired,* 12 February 2016. Available at: http://www.wired.co.uk/news/archive/2016-02/17/tim-cook-apple-encryption-iphone-san-bernardino and Kieren McGarthy, 'French, German ministers demand new encryption backdoor law', *The Register*, 24 August 2016. Available at: http://www.theregister.co.uk/2016/08/24/french_german_ministers_call_for_new_encryption_backdoor_law/ (last visited on 10 October 2016).

24 For analysis of the trend in public-private policing, see Garland 2001 and Ericson & Haggerty 1997.

25 See also Fijnaut in: Groenhuijsen & Knigge 2002, p. 689-749, Nuis et al. 2004, and the discussion document regarding the general provisions for pre-trial investigations (6 June 2014), p. 37-38. Available at: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/herziening-van-het-wetboek-van-strafvordering (last visited on 11 February 2016).

nal prosecution and the mechanisms that ensure transparency in the use of investigative methods by law enforcement officials in criminal investigations, are also not examined.

It is arguable that regulations for investigative methods are only effective when law enforcement officials respect them. In criminal procedural law, remedies can be provided to suspects for procedural defects that are caused by law enforcement officials. Remedies aim to show law enforcement authorities that investigations do not benefit from disregarding the regulations for investigative methods and that authorities must take procedural regulations seriously. This interest is balanced against the public interest not to leave criminal behaviours unpunished (cf. Keulen & Knigge 2010, p. 523-524).[26] In the Netherlands, trial judges can apply a remedy for procedural defaults with regard to the application of investigative methods.[27] The question whether these Dutch regulations for remedies find the right balance is not considered in this study, since it is related not only to art. 8 ECHR but rather to art. 6 ECHR.

The *regulation* of the investigative methods themselves is placed at the forefront of this study. It means that, although all aspects of art. 8 ECHR will be examined, the core of that provision as it pertains to the requirements of regulations is the primary focus in this study.

1.4 Research methodology

Four methodologies are used to answer the research questions: (1) desk research, (2) comparative legal research, (3) fieldwork, and (4) analysis. These methodologies are briefly discussed below.

1.4.1 Desk research

As applied in this study, desk research consists of scrutinising available scientific literature concerning the following five topics: (a) cybercrime, (b) the application of investigative methods in cybercrime investigations, (c) the relationship between the right to privacy and investigative methods, (d) the regulation of investigative methods in Dutch criminal procedural law, and

26 See for further reading, e.g., Embregts 2003, Van Woensel 2004, Keulen & Knigge 2010 and Borgers 2012.

27 In the Netherlands, the following remedies can be applied: (1) the determination a procedural defect has occurred (without imposing further sanctions), (2) the reduction of the imposed sentence, (3) the exclusion of evidence, and (4) the barring further prosecution of the suspect. The first remedy is created in case law (see, most notably, HR 30 March 2004, ECLI:NL:HR:2004:AM2533, par 3.6.1). The last three remedies are codified in art. 359a(1) DCCP. To decide which sanction is most appropriate, a trial judge must take into account the (1) interests served by the rule that is not observed, (2) the damage resulting from the noncompliance, and (3) the seriousness of the noncompliance for the suspect (art. 359a(2) DCCP).

(e) the territorial limits of enforcement jurisdiction. Desk research is thus applied in order to answer all five research questions.

In addition, desk research is applied to analyse Dutch regulations, legislative history, and jurisprudence regarding the identified digital investigative methods. Finally, news articles are examined and cited where they may shed light on the application of investigative methods in cybercrime investigations.

1.4.2 Comparative legal research

Comparative legal research is conducted in relation to the legal systems of the Netherlands and the United States.[28] This research method is used in order to examine the two countries' approaches to both the regulation of digital investigative methods and the principle of the territorial limitation of enforcement jurisdiction. Comparative legal research is primarily used for answering the fifth research question. Choosing the United States for study is part of the research methodology. The United States is chosen for this legal comparison for three reasons.

(1) The U.S. federal law enforcement agencies are frontrunners in the investigation and prosecution of cybercrime. The U.S. Federal Bureau of Investigation (FBI), the U.S. Secret Service, the U.S. Drug Enforcement Agency (DEA), and the U.S. Immigration and Customs Enforcement (ICE) have been particularly active in pursuing more 'high-tech' criminals, even when those suspects live outside the territorial borders of the United States.[29] The experience of U.S. law enforcement agencies can thus provide interesting insights, both in terms of practice and legal regulation.

(2) Knowledge about U.S. federal regulations may be important for Dutch law enforcement agencies and citizens, as many Dutch citizens make use of U.S. online services, such as Facebook, Gmail, Twitter, and LinkedIn. Therefore, Dutch law enforcement officials may be required to gather data on U.S. territory. Knowledge about U.S. law may assist them in gathering evidence on U.S. territory.

---

28 I was a visiting scholar of George Washington University from 5 September to 25 November 2011. This visit enabled me to study materials available in the United States and to speak with experts on digital investigations from the law enforcement and academic community.

29 The FBI is the largest federal organisation in the U.S. that handles computer crimes. Other federal agencies focus on specific crimes. The U.S. Secret Service particularly deals with financial fraud, such as the illegal online trade of credit card data. The DEA focuses on the illegal drug trade, and ICE conducts criminal investigations with regard to child abuse offences.

(3) The United States has a different approach toward the territorial limitation of enforcement jurisdiction than States in continental Europe, including the Netherlands. Past criminal investigations on money-laundering offences and drug-related offences have shown that U.S. law enforcement authorities are willing to intrude on the territory of sovereign States and override local legal norms in the pursuit of suspected criminals abroad (cf. Nadelmann 1993, p. 472-473). The different approaches of the Netherlands and the United States, as they pertain to the territorial limitation of enforcement jurisdiction, deserve further examination within the context of the cross-border unilateral application of digital investigative methods.

The Netherlands and the United States have rather different legal systems. The Netherlands has a civil law system; the United States has a common law system. Most notably, U.S. criminal procedural law is not bound by a criminal procedural legality principle as it is in the Netherlands. Instead, as in other common law States, the decisions of the Supreme Court of the United States are particularly important to U.S. criminal procedural law (cf. LaFave et al. 2009b, p. 3). There is thus not necessarily a broad set of statutory laws available to regulate investigative methods in the United States. In contrast, intrusive investigative methods in the Netherlands are regulated in detail within criminal procedural statutory law.

Due to the global nature of cybercrime and the similar challenges faced by law enforcements authorities in both States, a functionalist approach is appropriate for this legal comparison (cf. Gordely in: Monateri 2012). The starting point of the legal comparison is thus the equivalent function of the regulations and concepts. This approach is used with the aim of determining how the selected investigative methods are regulated in both the Netherlands and the United States and to examine each State's approach to the principle of the territorial limitation of enforcement jurisdiction.

1.4.3 Fieldwork

Fieldwork is necessary for gaining a better understanding of both cybercrime and the investigative methods utilised in cybercrime investigations. The fieldwork conducted for this study aims to fill knowledge gaps about the application and regulation of investigative methods in cybercrime investigations as well as to validate the findings of the desk research. The results of the fieldwork are therefore used to inform the findings for all five research questions. The fieldwork consists of (1) semi-structured interviews and (2) an analysis of police reports in criminal trial dossiers (i.e., dossier research).

Semi-structured interviews were conducted with 14 individuals with expertise in digital investigations. A combination of experts in a variety of fields were chosen. They have (a) expertise on technical aspects of digital investigative methods, (b) law enforcement experience in cybercrime investigations, or (c) knowledge of the theoretical background of the legal basis

for investigative methods. Thus, respondents in the relevant fields – technical, legal, and law enforcement – were chosen. Appendix A provides an overview of the individuals who were interviewed.

The dossier research consists of reviewing 10 case files at the High-Tech Crime and Telecommunications Department of the Dutch Public Prosecution Service. These case files were selected because they contain police reports that describe the application of digital investigative methods. The reports are analysed to determine which legal provisions law enforcement officials base the use of digital investigative methods on. In addition, the dossier research aims to establish what obstacles often arise in cybercrime investigations and how law enforcement officials handle these challenges by applying certain investigative methods. Prior permission to analyse the dossiers was obtained from the Research and Documentation Centre of the Dutch Ministry of Security and Justice. No permission was given to this researcher to copy any materials from the examined dossiers. Moreover, prior authorisation from the coordinating public prosecutor has been required for any references made to the examined case files.

1.4.4 Analysis

The results of different research methodologies are triangulated in order to answer the research questions. Triangulation means that the findings of the (1) desk research, (2) comparative legal research, and (3) fieldwork are compared to validate their results. This approach is suitable for the hybrid approach applied, which aims to provide an overview of legal frameworks and identify the misalignments that can occur in the practice of applying digital investigative methods within these frameworks. The results of the analysis provide important input for improving the relevant legal frameworks.

1.5 Structure of the thesis

An overview of the structure of this thesis follows.

Chapter 1 has introduced the subject of the thesis and formulated both the problem statement and research questions. The restrictions imposed on the scope of the research scope were also discussed, as were the research methodologies. Finally, this chapter presents the structure of the thesis.

Chapter 2 answers RQ 1 by explaining how evidence is gathered in cybercrime investigations. It examines how computers and the Internet facilitate crime and subsequently influence criminal investigations with regard to cybercrimes. In addition, the challenges of cybercrime investigations and their influences on the use of investigative methods are examined. The chapter also identifies the investigative methods that are commonly used in cybercrime investigations.

Chapter 3 answers RQ 2 by examining the normative requirements that can be derived from art. 8 ECHR for the regulation of investigative methods.

Chapter 4 answers RQ 3 by determining the gravity of the privacy interference that is caused by applying the identified digital investigative methods. Depending on the gravity of the privacy interference, a framework is proposed for requirements for the regulation of digital investigative methods.

Chapter 5 answers RQ 4a by investigating whether the gathering of publicly available online information is adequately regulated within Dutch criminal procedural law.

Chapter 6 answers RQ 4b by examining whether the issuing of data production orders to online service providers is adequately regulated by Dutch criminal procedural law.

Chapter 7 answers RQ 4c by testing whether the domestic legal framework for applying online undercover investigative methods is adequately regulated by Dutch criminal procedural law.

Chapter 8 answers RQ 4d by investigating whether the applicable regulations for performing hacking as an investigative method is adequately regulated by Dutch criminal procedural law.

Chapter 9 examines the international dimension of the application of digital investigative methods in cybercrime investigations. The extent to which evidence-gathering activities can be applied unilaterally across State borders is examined for each of the selected investigative methods. The analysis thus provides an answer to RQ 5.

Chapter 10 evaluates the previous chapters. Both the domestic and international legal frameworks are assessed to determine the steps that can be taken forward to legitimately and successfully investigate cybercrime.

Chapter 11 answers the problem statement. It presents the findings of this study and provides recommendations for improving the regulation of the investigative methods that are utilised in cybercrime investigations.

2 Digital investigative methods

This chapter aims to answer the first research question (RQ 1): *Which investigative methods are commonly used in cybercrime investigations?* For this purpose, the technicalities of evidence-gathering activities and the challenges of cybercrime investigations are analysed. The analysis provides a basic understanding of how digital investigative methods are used in practice. The following three-step approach is taken to answer the research question.

In the first step, the object of cybercriminal investigations, namely cybercrime, is examined. The aim is to construct a basic understanding of how computers and the Internet facilitate crime. Knowledge about cybercrime is important to the understanding of how cybercrimes are investigated.

In the second step, digital leads that law enforcement officials must often follow in cybercrime investigations are examined. These digital leads are identified as (1) IP addresses and (2) online handles.[1] Subsequently, the digital investigative methods that are used to gather evidence are based on these two digital leads in cybercrime investigations.

In the third step, three challenges in cybercrime investigations are examined. These challenges are (1) anonymity, (2) encryption, and (3) jurisdiction. These three challenges have already been separately identified and briefly analysed in other literature.[2] Based on the examination of case law, the dossier research, and the conducted interviews, it became clear that these three challenges often influence the course of the investigation. Further analysis of the challenges in cybercrime investigations is required, because law enforcement authorities deal with the challenges by using novel investigative methods. The identification of digital investigative methods used in cybercrime investigations is the aim of RQ 1.

---

1 These two digital leads were chosen based on the examined literature, case law, and dossiers.

2 See most notably: Franken 2004, p. 406 in: Franken, Kaspersen & De Wild 2004. See also for a similar distinction: Europol 2015b, p. 9: *"The main investigative challenges for law enforcement are common to all areas of cybercrime: attribution, anonymisation, encryption and jurisdiction"*. Note that operational challenges to investigate cybercrime are not examined in this study. Factors such as the scarcity of the right technical expertise within police organisations to use digital investigative methods also make it difficult to effectively investigate cybercrime. See, e.g., Wall 2007, p. 160-161, Brenner 2010, p. 162-172, Koops 2010 in: Herzog-Evans 2010, p. 740-741, Struiksma, De Vey Mestdagh & Winter 2012, p. 55, Stol, Leukfeldt & Klap 2012, p. 25-27, and Stol, Leukfeldt & Domenie 2013, p. 78. The premise of this study is that law enforcement authorities have the capacity and right expertise to investigate cybercrime.

The structure of this chapter follows these three steps. Section 2.1 addresses the first step and provides a definition and brief typology of cybercrime. The section further investigates how computers and the Internet facilitate these criminal behaviours. The second step is addressed in section 2.2, which examines how law enforcement officials gather evidence based on the digital leads of IP addresses and online handles. The third step is addressed in the sections 2.3 to 2.5. The three challenges of (1) anonymity, (2) encryption, and (3) jurisdiction are separately examined in order (a) to illustrate how the challenges influence cybercrime investigations and (b) identify which investigative methods are used to overcome the challenges in cybercrime investigations. Finally, section 2.6 concludes the chapter with a summary of the findings.

2.1 Cybercrime as the object of a criminal investigation

The term 'cybercrime' is broadly accepted in literature and has been adopted by the Council of Europe in the Convention on Cybercrime (cf. Clough 2010, p. 9).[3] The term 'cybercrime' is preferred in this study over the term 'computer crime', because the prefix 'cyber' emphasises that both computers *and* the Internet are inextricably linked with the crime. Cybercrime is defined in this study as *"criminal acts committed using electronic communication networks and information systems or against such networks and systems"*.[4] Based on this definition, cybercrimes can be distinguished as:

(1) target cybercrimes: crimes in which a computer is the target of the offense; and
(2) tool cybercrimes: crimes in which a computer is used to facilitate a traditional crime.[5]

This section provides a brief typology of target cybercrimes and tool cybercrimes in subsections 2.1.1 and 2.1.2.[6] Knowledge about both types of cybercrime is required, in order to understand how computers and the Internet are used to commit such crimes and how this subsequently influences cybercrime investigations.

3 Council of Europe, Convention on Cybercrime (ETS No. 185). Adopted on 8 November 2001 in Budapest. Kaspersen (2007, p. 180-182 in: Koops 2007) noted that this convention is the most influential international treaty related to cybercrime.

4 See Communication of 22 May 2007 from the European Commission, 'Towards a General Policy on the Fight against Cybercrime', COM(2007)267 final, p. 2.

5 See also subsection 1.3.1.

6 These are generic descriptions of cybercrimes that do not necessarily correspond to the national crime depiction of the behaviours in criminal substantive law. The exact content of the crime description may have an influence on the manner it may be investigated. The examination of criminal substantive law with regard to cybercrime goes beyond the scope of this study. See, e.g., Koops 2007 and Kerr 2010 for an analysis of criminal substantive law with regard to cybercrime in the Netherlands and United States.

2.1.1 Target cybercrimes

In target cybercrimes, the computer is the target of the offence. A computer is defined as: "*any device which electronically processes data, stores data, or transfers data*".[7] This definition of a computer encompasses a wide range of different types different types of devices.

For example, the following devices may be understood as computers: (a) PCs, laptops, smartphones, and wearable computing devices (e.g., 'Google Glass'), (b) 'web servers' that deliver web content for websites, and (c) all kinds of computing devices connected to the Internet such as routers, smart meters, and even household appliances and automobiles. All these types of computers are vulnerable to crimes that may endanger the (1) confidentiality, (2) integrity, or (3) availability of computers (cf. Schermer 2010).[8]

Three examples of target cybercrimes are (A) hacking, (B) the use of malware, and (C) the use of botnets. These three crimes are briefly discussed below to illustrate what target cybercrimes entail and how the Internet facilitates these offences.

A Hacking

Hacking is perhaps the best-known example of a 'target cybercrime'. In a criminal context, the term hacking refers to the act of intentionally gaining unauthorised access to computers (cf. Kerr 2010, p. 27). Computers can be hacked in numerous ways. Hacking a computer may be as straightforward as (a) copying a login name and password by looking over the shoulder of an unwary computer user ('shoulder surfing'), (b) posing as a system administrator to trick a person into giving up his[9] login name or password (a form of 'social engineering'), or (c) buying login credentials on an online black market and subsequently using those credentials to gain access to a service. In more technically advanced attacks, hackers exploit vulnerabilities in software in order to gain access to a computer system. Hacking is often used as a vehicle to perpetrate other target cybercrimes.

---

7 This definition resembles the definition for 'automated devices' in the art. 80sexies of the Dutch Penal Code. However, this definition is broader in nature, since the criteria are not cumulative in art. 80sexies Dutch Penal Code. The Dutch Computer Crime Act III aims to expand the definition for automated devices in art. 80sexies Dutch Penal Code (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 92-94).

8 In his article, Schermer (2010) identifies crimes that can be committed with regard to computers that are part of 'ambient intelligent services'. The concept of 'ambient intelligence', which is related to the concepts of 'ubiquitous computing' and 'the Internet of Things', is not considered in this study. See for analysis of these concepts: Greenwield 2006 and Atzoria, Ierab & Morabito 2010. See Goodman 2015 for an analysis of cybercrime in relation to the Internet of Things. See Pfleeger 2003, p. 504 in: Ralston, Reilly & Hemmendinger 2003 for an analysis regarding the elements of (1) confidentiality, (2) integrity, and (3) availability.

9 For readability, 'he' and 'his' are used wherever 'he or she' and 'his or her' are meant.

The Internet facilitates hacking by allowing criminals to gain unauthorised access to computers on a global scale. In target cybercrimes, there is no physical proximity between the perpetrator and the victim of the crime (see Koops 2010, p. 740 in: Herzog Evans 2010).[10] As a result, the leads that law enforcement officials must follow are often digital in nature.

B The use of malware

In order to commit computer crimes, cybercriminals often make use of malicious software, known as 'malware'. Computers can be infected with malware in numerous ways. Malware is often distributed through (a) e-mails with a disguised infected attachment, (b) social media services that link to infected websites (suggesting access to the latest 'viral movie', for example), and (c) malicious advertisements on websites that attempt to exploit vulnerabilities on a computer system.

Malware enables cybercriminals to gain remote access to a computer and take control of the functionalities of a computer. For example, malware can be used to (a) control the user's cursor, (b) log keystrokes, (c) record video through a built-in web cam, (d) record sounds using a microphone in a computer, and (e) take screenshots of the computer screen. These functionalities of malware can be used to commit other cybercrimes.

Once the perpetrator has gained access to an infected computer, the data stored in a computer can be altered, copied, or deleted. Malware can therefore be used to (a) extort individuals by taking computer files hostage, (b) spy on individuals, (c) copy information from infected computers, and (d) direct infected computers to take certain actions. The compromised computer can also be used as a cover – a 'proxy' – to commit other crimes (cf. Clough 2010, p. 28-30).[11] Criminals continuously update malware in order to avoid security measures. These kinds of rapid innovation cycles are characteristic for cybercrime (cf. Koops 2010, p. 741 in: Herzog Evans 2010).

C The use of botnets

A botnet can be defined as a network of infected computers that is controlled by the perpetrator through a 'command-and-control' channel. Botnets can be visualised as follows.

10 Koops cites Yar 2005, p. 421 and Sandywell 2010 in: Jewkes & Yar 2010, p. 44 with regard to these two factors on how the Internet facilitates cybercrime.

11 See subsection 2.3.2 for more information about proxy services.

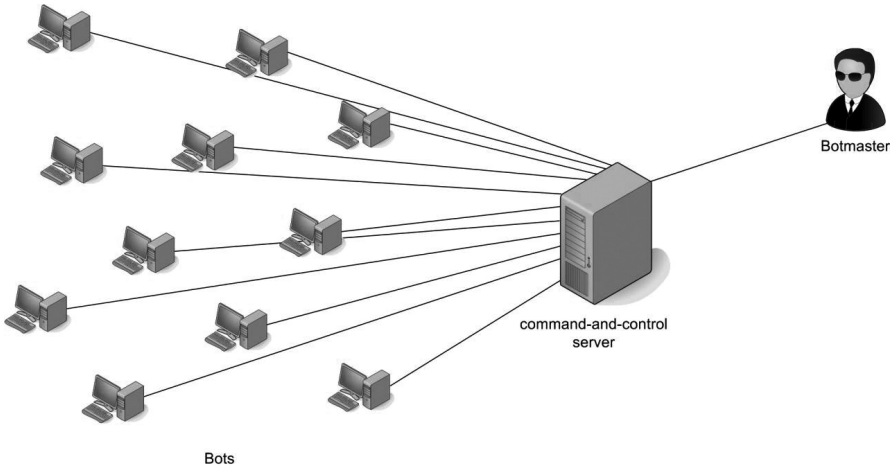

Figure 2.1: Model of a centralised botnet (see Hogben ed. 2011, p. 16).

Figure 2.1 depicts a model of a centralised botnet. It shows how all infected computers connect to one command-and-control server that is controlled by the perpetrator. In practice, the IT infrastructure of botnets is often more sophisticated in nature (see Hogben ed. 2011, p. 18-21). Criminals utilise botnets to commit other crimes, such as (a) sending large amounts of unsolicited e-mail (spam), (b) harvesting personal data (such as login names and passwords) from infected computers, (c) committing 'click fraud'[12], and (d) initiating 'denial of service attacks'[13] (see Hogben ed. 2011, p. 22-25). An organisation is required to commit these crimes and monetise the money that has been obtained by these crimes. A 'malware economy' has arisen following these target cybercrimes (see Van Eeten & Bauer 2008).

The use of botnets by criminals illustrates how computers and the Internet can facilitate crime in an automated process by remotely harvesting data obtained from infected computers (cf. Koops 2010, p. 740 in: Herzog Evans 2010). The use of botnets also illustrates how different target cybercrimes are often committed in conjunction with each other.

12 In click fraud cases, infected computers are directed to visit an advertisement. Criminals can earn money by directing infected computers to pre-selected advertisements.

13 'Denial-of-service attacks' can be characterised as an attack in which large amounts of data ('network traffic') are sent to a computer (usually a server) in order to overload that computer with traffic. As a consequence, websites or internet services facilitated by that server take more time to load and may appear unavailable.

2.1.2 Tool cybercrimes

In tool cybercrimes, computers and the Internet play an essential role, facilitating the commission of traditional crimes a number of ways. In short, criminals can take advantage of computers and the Internet to commit crimes relatively anonymously, across State borders, and even on a global scale, reaching many computer users (cf. Koops 2010, p. 740-741 in: Herzog Evans 2010).[14]

Three examples of crimes in which computers and the Internet are used as tools to commit crimes are (A) child pornography crimes[15], (B) online drug trafficking, and (C) online fraud. These three cybercrimes provide a good overview of how the Internet facilitates tool cybercrimes. They are briefly discussed below.

A Child pornography crimes

Child pornography crimes are a typical tool cybercrime. Child pornography can be defined as images or videos that depict minors engaging in sexual acts. In the past, child pornography was published in magazines and distributed by mail or bought 'under the counter' at kiosks. Since the 1990s, child pornography has predominately been distributed over the Internet (cf. Jenkins 2001).

Computers and the Internet facilitate the possession and distribution of child pornography by enabling child pornographers to access, download, upload, and distribute child pornography materials, without being in physical proximity to the victims (cf. Brenner 2010, p. 167-170). Child pornography users can distribute child pornography through a variety of internet related services, such as e-mail, chat applications, file transfer programs, and online forums (see Oerlemans 2010). The Internet facilitates perpetrators in a global reach by enabling them to target victims and collaborate with others anywhere in the world (cf. Yar 2005, p. 421).

B Online drug trafficking

Computers and the Internet can also facilitate drug trafficking. The Internet essentially provides criminals with a platform to communicate with each other and to trade in illegal goods and information (cf. Paretti 2009, p. 386, Bernaards, Monsma & Zinn 2012, p. 89-96). Specialised online trading forums allow individuals to buy and sell drugs on a global scale. Below is a screen shot of the (now defunct) drug-trading forum 'Silk Road'.

14 Koops provides an overview on twelve ways the Internet facilitates crime, building upon the work of authors such as Brenner 2002, Yar 2005, Wall 2007, and Sandywell 2010 in: Jewkes & Yar 2010.

15 The term 'child pornography crimes' refer to the possession, import, export, distribution, fabrication, and access to child pornography.

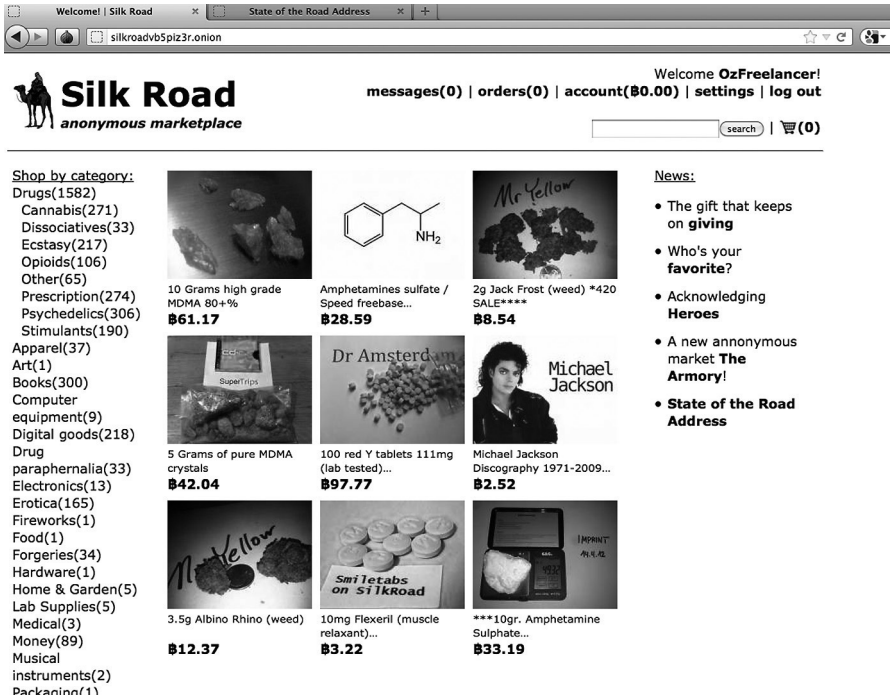

Figure 2.2: Screen shot of the Silk Road forum. Eileen Ormsby, 'The drug's in the mail', 27 April 2012, TheAge.com. Available at: https://allthingsvice.files.wordpress.com/2012/05/screen-shot-2012-04-24-at-2-02-25-am.png (last visited 30 September 2015).

Figure 2.2 illustrates how these forums bring together internet users that want to buy and sell (mostly) drugs. Silk Road was a very successful online black market that facilitated the trade in illicit goods and services, primarily drugs.[16] The U.S. prosecutor contended that during its 2,5 years in operation, Silk Road was used by several thousand drug dealers to distribute hundreds of kilos of drugs to over a 100,000 buyers. From those transactions, reportedly laundered hundreds of million ns of dollars were laundered through the forum.[17] The administrator of the forum obtained money by facilitating and withholding of a small percentage of the transactions between users of

16 The website gained popularity after an interview with the administrator of the forum, Ross Ulbricht, was published on the website Gawker (See Adrian Chen, 'The Underground Website Where You Can Buy Any Drug Imaginable', 1 June 2011, Gawker. Available at: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160 (last visited on 30 September 2015).

17 See p. 6 of the indictment of the United States against Ross Ulbricht. Available at: https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf (last visited on 30 September 2015).

the forum.[18] The increase of online black markets specialising in drug trafficking in the last five years, illustrates how the Internet provides a global platform for criminals to distribute illegal goods and services (cf. UNODC 2014, p. 18 and Europol 2015a, p. 31).[19] An important factor may also be that the Internet can provide (a degree of) anonymity when individuals make use of specialised services. This aspect is further examined in section 2.3.

C Online fraud

Clough (2010, p. 372-373) submits that online fraud is *"undoubtedly one of the most common forms of cybercrime"*. He argues that (1) the scale of potential victims, (2) the anonymity that the Internet provides to the perpetrators, and (3) the ease of communication are factors that facilitate fraudulent online scams. Indeed, most people are familiar with scams sent by e-mail with fraudulent investment opportunities or scams that aim to trick people into transferring funds. Online fraud is a rather broad category of tool cybercrimes, whilst it is often also closely linked to target cybercrimes.

An example that illustrates how online fraud is committed and how this tool cybercrime is intertwined with the commission of target cybercrimes follows hereinafter. In an online fraud scheme in which criminals use 'banking malware', criminals often send an innocent looking e-mail to victims that lure them into clicking on a link.[20] That link then directs the victim to a website that automatically downloads so-called banking malware on the computer system of the victim, insofar the victim's computer is vulnerable to the attack. When the victim attempts to electronically transfer funds from his online banking website, the banking malware turns into action and

18 See Pammy Olson, 'The man behind Silk Road – the internet's biggest market for illegal drugs', *The Guardian*, 10 November 2013. Available at: http://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht (last visited on 20 November 2015). After the arrest of the forum administrator, Ross Ulbricht, his laptop was seized. His laptop contained 144,336 bitcoins, a virtual currency worth more than 28 million dollars at the time. See the press release of the U.S. Department of Justice, 'Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road', 16 January 2014. Available at: http://www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php (last visited 30 September 2015.

19 See also Patrick Howell O'Neill, 'Dark Net markets offer more drugs than ever before', *The Daily Dot*, 15 May 2015. Available at: http://www.dailydot.com/crime/dark-net-census-growth-37-percent/ (last visited on 3 August 2015). For a recent example of online drug trading forums originating in the Netherlands, see: *ANP*, 'OM wil tot zeven jaar cel voor Internetdealers', *Nu.nl*, 23 September 2014. Available at: http://www.nu.nl/Internet/3885624/wil-zeven-jaar-cel-Internetdealers.html (last visited on 17 April 2015) and J.J. Oerlemans, 'Veroordelingen voor drugshandel via online marktplaatsen', *Computerrecht* 2015, no. 3, p. 170, relating to the cases of Rb. Midden-Nederland, 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792.

20 See, e.g., Rb. Rotterdam, 20 July 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m.nt. J.J. Oerlemans. Note that many more attack methods are available to criminals.

instead transfers money to a different recipient (cf. Sandee 2015).[21] Hence, online fraud (a tool cybercrime) has taken place with the aid of hacking and malware (a target cybercrime).

Note that the criminals who create malware or hack computers to steal information are not necessarily the same people who monetise the information. Furthermore, the process of hacking and monetising the stolen data is highly organised. Criminals often have different professional roles assigned to them in order to deal with the different economic and technical aspects of the crimes.[22] Cross-border online crime groups are often fluid and temporal in nature. In other words, the Internet also permits perpetrators to loosely organise themselves in order to (a) divide labour and (b) share skills, knowledge, and tools to commit crimes (cf. Koops 2010, p. 740 in: Herzog Evans 2010).[23]

2.2 Digital leads

The illustration of target cybercrimes and tool cybercrimes in section 2.1 has shown that cybercrimes can be committed on a large (global) scale, across State borders, reaching many computer users. The investigation of target cybercrime and tool cybercrimes have in common that – at the start of the investigation – there are no physical leads available. The examined literature, case law, and dossiers show that the only leads that are often available in cybercrime investigations are (1) IP addresses and (2) online handles.

An *Internet Protocol address* is a numerical address that is assigned to a computer, which is part of a computer network and makes use of the Internet Protocol to communicate. Internet access providers also assign an IP address to the network device that computers use to access the Internet. For example, the (public) IP address assigned to the network device that this author's working station is connected to at Leiden University is '132.229.159.109'. IP addresses usually consist of four sets of numbers between 0 and 255.[24] As a digital lead, IP addresses often do not specifically identify the device that an individual utilises, but they do provide law enforcement officials with a clue about the particular network that a person uses for his internet connection. Law enforcement officials can attempt to

21 Sandee describes in his report how the popular type of banking malware, called ZeuS, infected computers and siphoned money of the online bank accounts of its victims. The report also describes the sophisticated organisation behind the malware.

22 See, e.g., Hogben ed. 2011, p. 21, Soudijn & Zegers 2012, p. 114-115 and Sandee 2015.

23 See for further analysis, e.g., Brenner 2002, p. 45-47, Choo 2008, p. 276, McCusker 2006, p. 267, Paretti 2009, p. 398, Soudijn & Zegers 2012, p. 114-115 and Europol 2015a.

24 This is only true insofar the IP address uses the IP protocol version 4 (IPv4). Steadily, IP addresses with IP protocol version 6 (IPv6) replace IPv4. The transition from IPv4 to IPv6 will impact digital investigations (cf. Bernaards, Monsma & Zinn 2012, p. 135-136). An analysis of the manner in which the transition to IPv6 impacts cybercrime investigations is beyond the scope of this study.

identify a computer user by requesting or ordering the disclosure of data from the organisation or person that has information about the devices and computer users within a network. The investigation process based on IP addresses as a digital lead is further explained in subsection 2.2.1.

An *online handle is* a name an individual uses to interact with other individuals on the Internet. An online handle may be the real name of an individual. On the Internet, it is also common to use pseudonyms, called 'nicknames', as online handles when communicating with other people. Nicknames are often used on online discussion forums or chat channels. Online handles can also consist of the first part of an e-mail address and profile names on social media services. Online handles are a digital lead for three reasons. They (1) can allow law enforcement officials to gather publicly available information about an internet user, (2) can direct law enforcement officials to an online service provider that may hold information about an internet user, and (3) can enable law enforcement officials to interact (undercover) with the individual. The investigative process based on online handles in cybercrime investigations is further explained in subsection 2.2.2.

This section (section 2.2) thus examines the two digital leads that law enforcement officials follow in cybercrime investigations and the investigative methods that law enforcement officials subsequently use to gather evidence. Creating a clear understanding of the actual – technical – acts involved therein will create a basis for the analysis of digital investigative methods (with their accompanying legal frameworks), which will be analysed in the following chapters.

2.2.1 Tracing back an IP address to a computer user

As explained in the introduction of this section, public IP addresses do not specifically identify the device that an individual utilises. However, they do provide law enforcement officials with a clue about the particular network that a person uses for his internet connection. Figure 2.3 illustrates how computers in a residence are connected to the Internet by a network connection device, such as a router.[25]

25 A router 'routes' traffic by cable or WiFi to a connected computer.

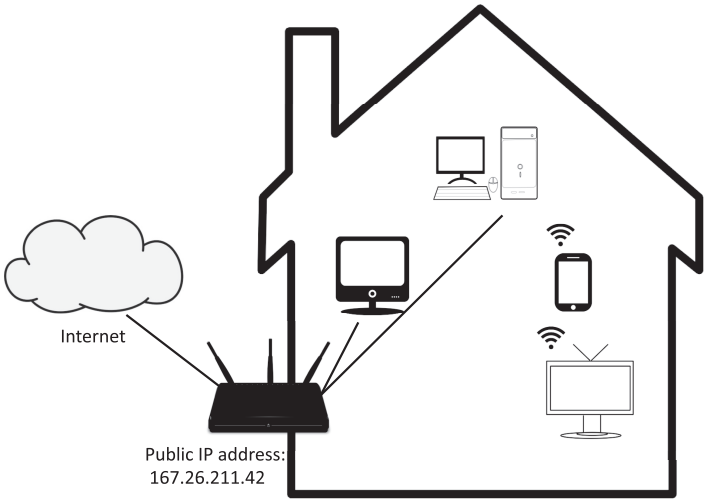

Figure 2.3: Simplified model of a residential internet connection.

Tracing back a computer user on the basis of an IP address as a digital lead can take place as follows. Imagine that in a criminal investigation related to a hacking case, an IP address is available because detection systems logged a suspect IP address at the time the hacking incident occurred. As illustrated above, the logged IP address could be the 'public IP address' of a router, distributing a broadband internet connection to the devices that members of a household utilise to access the Internet. Using publicly available services, law enforcement officials can often find the organisation to which that specific IP address is assigned.[26] In the event that an internet access provider allocates the IP address to a subscriber, law enforcement officials can send a *data production order* to an internet access provider to identify the customer. A data production order requires the custodian of data to deliver or make data available to law enforcement authorities within a specified period. Internet access providers usually retain logs of the IP addresses assigned to customers for billing and security purposes. As a result, internet access providers are often able to provide the identity of the subscriber that has been assigned a specific IP address to law enforcement authorities.

Using the name and address information that belong to a subscriber, law enforcement agents may be able to locate the suspect.[27] To establish a link between (1) the crime, (2) the IP address, and (3) the suspect, the application of additional investigative methods – such as performing a digital forensic analysis of a router distributing the internet connection and interviewing

26 Visit, for example, http://whois.domaintools.com and type in '132.229.159.109' to trace the IP address to the company or institution that allocated it. The query will unsurprisingly return contact data from Leiden University (last visited 19 January 2014). However, the information is often not up-to-date or accurate.

27 See for a more extensive analysis Clayton 2004, p. 17-25.

members of the household – may be required. Information that is available on seized computers can also provide law enforcement authorities with further evidence of a crime.

The above example represents an ideal situation for law enforcement officials, i.e., when an IP address is allocated by an internet access provider and directly relates to the residential internet connection that a suspect uses. However, even in that ideal situation, law enforcement officials still need to take several steps (and have to invest considerable time and energy in the process) to prove that the suspect used the identified computer when the crime was committed. Nevertheless, the digital lead in the form of an IP address will often be an indispensable starting point.

2.2.2 Online handles

As explained in the introduction of section 2.2, online handles can enable law enforcement officials to identify an internet user in three different manners.[28] Online handles can (1) allow law enforcement officials to *gather publicly available information* about an internet user, (2) can direct law enforcement officials to an online service provider and information about internet users with *data production orders*, and (3) can enable law enforcement officials to interact with the individual that makes use of a particular online handle by using *online undercover investigative methods*. These three investigative activities of law enforcement officials are described below.

A Gathering publicly available online information

Online handles provide law enforcement officials with a lead to collect information about an individual that is publicly available on the Internet. Publicly available information can be defined as information that anyone can lawfully obtain (a) upon request, (b) through purchase, or (c) observation (cf. Eijkman & Weggemans 2012, p. 287).[29] The term 'publicly available information' is derived from article 32(a) of the Convention of Cybercrime and includes information provided by a third party that is only available after registration or payment.[30]

---

28 Note that the use of nicknames by criminals is common, as they will be inclined to hide their real identities (cf. Fabers 2010, p. 131-132). Cybercriminals often know each other only by nickname and may have never even met in real life (cf. Choo 2008, p. 277). Interviews with law enforcement officials and the dossier research conducted in the course of this research indeed showed that cybercrime suspects in those cases always use nicknames.

29 Eijkman &Weggemans refer to the National Open Source Enterprise, Intelligence Community Directive 301 of July 2006 for this definition.

30 Note how the Europol Decision of 2009 stipulates *"(...) Europol may directly retrieve and process data, including personal data, from publicly available sources, such as media and public data and commercial intelligence providers* (...)". See art. 25(4) of the Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/271/JHA), L 121/51.

An online handle may in itself provide the information required to identify a suspect. It may also be the beginning of a 'digital trail' that may be followed as individuals use the Internet. Such trails may include information about individuals who are of interest to a criminal investigation that is posted by *other* internet users.

In this study, the gathering of publicly available online information as an investigative method is further distinguished as: (A1) the manual gathering of online information, (A2) the automated gathering of publicly available online information, and (A3) the observation of the online behaviours of an individual. These types of gathering publicly available online information as an investigative method are examined below.

A.1 Manual gathering of online information

Law enforcement officials can manually gather publicly available online information. In its most elementary form, the investigative method consists of a law enforcement official looking for information about a person on the Internet by typing in key words on an internet search engine, such as Google. Information that is publicly available online can be gathered from a wide variety of sources, including: (a) websites open to the general public, (b) social media websites, (c) online phone directories, (d) discussion forums and blogs, (e) news articles, and (f) commercial or scientific reports (cf. Carter 2009, p. 285).

A.2 Automated gathering of publicly available online information

Information that is publicly available on the Internet can also be collected using automated data collection systems. Law enforcement authorities have an interest in making large amounts of online data available to them and making use of the available data as efficiently as possible.[31] Against that background, software has been developed for this purpose that essentially 'vacuums' relevant information from publicly available sources on the Internet and pre-emptively stores that information in police systems. That way, the information can be made accessible to law enforcement officials later in time. For instance, so-called 'crawler' and 'spider' software automatically look for relevant information on the Internet based on certain parameters, such as certain search terms or images (cf. Lodder et al. 2014, p. 70). 'Scraper' software can also automatically download the online data onto computer systems. Automated data collection systems can find information on the Internet more efficiently and provide information to law enforcement officials more effectively.

31 For instance, the Dutch iColumbo system reportedly aims to provide *"an 'intelligent, automated, "near" real-time Internet monitoring service' for governmental investigators"*. See 'Deelprojectvoorstel, Ontwikkeling Real Time Analyse Framework voor het iRN Open Internet Monitor Network', 'iColumbo'. Available at http://www.nctv.nl/Images/deel-projectvoorstel-ontwikkeling-icolumbo-alternatief_tcm126-444133.pdf (last visited on 23 December 2015).

Koops (2013, p. 655) highlights that automated data collection systems may include advanced options, such as: *"plug-ins that enhance the search and analysis capacities of Internet searches, for example, through entity recognition, image-to-image conversion, and automated translation"*. Commercial services that automatically collect and analyse publicly available online information are also available to law enforcement authorities. For example, the Dutch company 'Obi4Wan' collects information from more than four hundred thousand internet sources every day in order to provide 'online monitoring' solutions.[32] Law enforcement can also obtain a quick overview of a suspect's social media network by using tools that map out an individual's friends on social media profiles. Internet monitoring systems can also harvest relevant information for extended periods of time, enabling law enforcement officials to create a timeline of an individual's online behaviours or online communications. Once the information is harvested, individuals can no longer delete online posts or alter information to prevent others from acquiring the information. All publicly available information that a suspect or other individuals post online is theoretically available to law enforcement officials in a criminal investigation.

A.3 Observing online behaviours of individuals

Law enforcement officials may also observe the behaviours of individuals on publicly accessible places online based on an online handle. For instance, law enforcement officials can take detailed notes about public posts that an individual makes on online services such as social media services, online forums, and chat services.

Similar to visual surveillance in the physical world, this investigative method allows law enforcement officials to learn more about the individual involved in the criminal investigation by observing his online behaviours. The observation of an individual's online behaviours can be regarded as the digital equivalent of the investigative method of 'visual observation' in the physical world.

The difference between the manual gathering of publicly available online information and the observation of online behaviours is that the manual gathering regards *information that has already been published* by individuals, and the observation of online behaviours concerns *new information that is being generated by individuals*.[33]

32 See http://www.obi4wan.com/online/social-media-monitoring/ (last visited on 19 September 2015). Although the service is mainly advertised to be useful for 'reputation management', the service also ensures that relevant information that has been posted online is available for further analysis. According to their website, Obi4Wan counts the Dutch national police as one of their clients.

33 See for a similar distinction CTIVD 2014, p. 9 and p. 42.

B Data production orders

Online handles can also provide a lead to an online service provider that stores information about an individual that may be of interest to law enforcement authorities. For instance, an online handle that consists of an e-mail address that ends with '@gmail.com' is obviously from the popular webmail service offered by Google, Gmail. In that event, law enforcement authorities may be able to obtain data of a specific account holder at Gmail with a data production order issued to Google. As explained in subsection 2.2.1, a data production order requires the custodian of data to deliver or make data available to law enforcement authorities within a specified period.

Many different types of structured and unstructured data (e.g., account information, traffic data, and stored documents) are stored and processed by third parties. This study focuses on data production orders that are issued to online service providers, since these providers often provide important evidence in cybercrime investigations. Data production orders that are issued to online service providers can be divided into the following four categories: (1) subscriber data, (2) traffic data, (3) other data, and (4) content data. The categorisation is largely based on the distinctions made with regards to production orders in the Convention on Cybercrime.[34] The four categories of data production orders are further examined below.

The first category, subscriber data, relates to subscriber data from online service providers. The category of subscriber data entails the following data: (a) the type of communication service used, the technical provisions taken, and the period of service, (b) a subscriber's name, postal or geographical address, telephone number, billing and payment information, and (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.[35] Subscriber data can thus be used to identify a suspect based on such information.

The second category, traffic data, consists of data that is generated by a computer system as part of the chain of communication. Traffic data can reveal the following information about a communication: origin, destination, route, time, date, size, duration, and type of underlying service.[36] Law enforcement officials can obtain valuable evidence by analysing network traffic data (cf. Oerlemans 2012, p. 31).[37] Traffic data may enable law enforcement officials to learn about (a) the device that a suspect uses, (b) the internet services that a suspect is using at a specific time, and (c) the suspect's device's location data.

---

34 Council of Europe, Convention on Cybercrime (ETS No. 185). Adopted on 8 November 2001 in Budapest. See art. 16-18 of the Convention on Cybercrime.

35 Art. 18(3) Convention on Cybercrime.

36 Art. 1(d) Convention on Cybercrime.

37 See also the analysis of Nicolas Weaver in the article of Paul Rosenzweig, 'iPhones, the FBI, and Going Dark', 4 August 2015. Available at: https://www.lawfareblog.com/iphones-fbi-and-going-dark (last visited on 18 August 2015).

The third category, other data, is not identified in the Convention on Cybercrime. The category of 'other data' is data that is not subscriber data, traffic data, or content data (which will be described below). For example, other data can consist of individuals' profile information that may depict information such as the date of birth, relationship status, sexual orientation, and political views, which may be available at social media providers. Profile information can aid law enforcement officials in gathering more information about the background and network of individuals surrounding an individual.

The fourth category, content data, is named but not explicitly defined in the Convention on Cybercrime. Content data is 'data with regard to the meaning or message conveyed by the communication, other than traffic data'.[38] This category of data consists of private messages that can be sent using online service providers. Arguably, the category also entails stored documents that are available from online storage providers. Law enforcement officials can gather content data from online service providers with data production orders. This data may provide them with evidence about the crime that is under investigation, but can also enable them to learn about a suspect and his surroundings, which can influence the use of other investigative methods (see Odinot et al. 2012, p. 91-94).

C Online undercover investigative methods

An online handle can provide law enforcement officials with an opportunity to interact with the individuals involved in a criminal investigation. When a suspect or an individual that has valuable information for law enforcement authorities is active on a social media service, law enforcement officials can interact with that individual on the Internet. For instance, law enforcement officials can add themselves to a suspect's network by introducing themselves as 'friends' of the suspect. These activities can be identified as *online undercover investigative methods*.

The distinguishing feature of undercover investigative methods, as compared to other investigative methods, is that law enforcement officials *interact* with other individuals – using a fake identity – in order to gather evidence in a criminal investigation (cf. Marx 1988, p. 11-13 and Kruisbergen & De Jong 2010, p. 239). In this context, a fake identity means that they do not reveal that they are law enforcement officials. In undercover investigations, suspects are both unaware of the purpose and the identity of the undercover agents (cf. Joh 2009, p. 161). Although this study focuses on evidence-gathering activities by law enforcement officials, it is important to point out that civilians can be recruited by law enforcement authorities to act as informants and to collect information about suspects in criminal investigations. In an online context, this provides law enforcement officials with the opportunity to request an informant's login credentials and to use

38 Explanatory memorandum Convention on Cybercrime, par. 209.

his online account to gain access to otherwise private information.[39] For example, with access to the online account of an informant, law enforcement officials can view content that is only accessible to members of an online forum. Informants can also be instructed to interact with other individuals and to log those communications for law enforcement officials.

Online undercover investigative methods that are applied by law enforcement officials can be distinguished in the following investigative methods, which are commonly used in cybercrime investigations: (1) online pseudo-purchases, (2) online undercover interactions, and (3) online infiltration operations.[40]

The first undercover investigative method, performing an online pseudo-purchase, can best be described as a scenario in which an undercover law enforcement official poses as a potential buyer of an illegal good in order to gather evidence of a crime. For example, law enforcement officials can buy drugs from a drug dealer to gather evidence in a criminal investigation. In a similar way, law enforcement officials can, for instance, buy stolen data and weapons from vendors in online forums in order to collect evidence in a cybercrime investigation.[41]

The second undercover investigative method, performing online undercover interactions with individuals, can take place on many online services, such as chat services, private messaging services, social media services, online discussion forums, and online black markets.[42] With the right knowledge of internet subcultures, law enforcement officials can interact and build relationships with individuals under a credible, fake identity in order to gather evidence in criminal investigations (cf. Siemerink 2000b, p. 145 and Petrashek 2010, p. 1528).

---

39 Problems may arise when law enforcement officials make use of an individual's existing personal information, such as a profile photo of a social media service or a name of an individual, without consent. See, e.g., the following quote in a news article covering a high-profile case in which the DEA used personal information of suspect for investigation purposes: "*After her cellphone was confiscated when she was arrested, a DEA agent named Timothy Sinnigen used the photos on her phone, including images of Arquiett in her skivvies and Arquiett with her son and niece, to create a profile page in her name so he could contact people he suspected of being involved with drugs*" (Kate Knibbs, 'DEA Used a Woman's Private Photos to Catfish Drug Dealers on Facebook', *Gizmodo*, 20 January 2015. Available at: http://gizmodo.com/doj-will-pay-134k-for-catfishing-drug-dealers-with-wom-1680743269). The woman involved successfully sued the U.S. Justice Department and settled for 134,000 dollars.

40 This distinction is used in Dutch criminal procedural law and has been identified in the examined case files.

41 See, e.g., Arrondissementsparket Amsterdam, 'Pseudokoop wapen met bitcoins door politie en OM', 17 January 2014. Available at: https://www.om.nl/vaste-onderdelen/zoeken/@32570/pseudokoop-wapen/ (last visited on 17 March 2016).

42 See, e.g., Landelijk Parket, 'Undercover onderzoek naar illegale marktplaatsen op Internet', 14 February 2014. Available at: https://www.om.nl/@32626/undercover-onderzoek/ (last visited on 17 March 2016).

The third undercover method distinguished in this study is performing an online infiltration operation. Infiltration operations are similar to undercover interactions with individuals. However, infiltration operations are characterised by the fact that undercover agents are authorised (to a certain extent) to participate in a criminal organisation in order to maintain cover and to gain a targeted individual's trust in a criminal investigation (cf. Joh 2009, p. 166). In infiltration operations, law enforcement officials can *participate* in a criminal organisation in order to gather evidence in a criminal investigation and to gain access to the upper echelons of a criminal organisation (cf. Joh 2009, p. 167). These operations can also take place, for instance, through participation in a criminal organisation that is active on an online black market.

The following case is illustrative of a successful infiltration operation of an online black market. In 2006, the FBI conducted an innovative undercover operation on the online forum 'DarkMarket'.[43] DarkMarket was an online black market in which participants specialised in trading stolen credit cards. Access to the market was only provided through an introduction of another forum member. To infiltrate the forum, an FBI agent was provided a cover by the non-profit private organisation Spamhaus, which combats spam and other cybercrimes. With the cover of the made-up criminal 'Pavel Kaminski', reported by Spamhaus as a notorious Eastern European cybercriminal, access was granted by other forum members to the DarkMarket forum. Using the nickname of 'Master Splyntr', the undercover FBI agent was able to climb to the highest levels of the organisation behind the forum. The undercover agent identified other forum members by interacting with them online. The FBI agent also secretly sent network traffic from the forum to a computer of the FBI that logged the IP addresses associated with all the forum's registered members. Ultimately, the FBI arrested fifty-eight individuals and proclaimed it had prevented seventy million dollars in damage.[44] The FBI concluded that: "*what's worked for us in taking down spy rings and entire mob families over the years -embedding an undercover agent deep within a criminal organization – worked beautifully in taking down Dark Market*".[45] Even after a decade, this online undercover operation is still exemplary for its successful use of the investigative method of infiltration on the Internet.

43 The summary of the DarkMarket investigation is based on the books from Misha Glenny, *DarkMarket: CyberThieves, CyberCops and You*, London: Bodley Head 2011 and Kevin Poulson, *Kingpin. How one hacker took over the billion-dollar cybercrime underground*, New York: Crown Publishers 2011.

44 See the FBI press release "Dark Market' Takedown Exclusive Cyber Club for Crooks Exposed', 20 October 2008. Available at: http://www.fbi.gov/news/stories/2008/october/darkmarket_102008 (last visited on 22 July 2015). The FBI was probably able to prevent damages by informing credit card companies of stolen credit card credentials.

45 See the FBI press release "Dark Market' Takedown Exclusive Cyber Club for Crooks Exposed', 20 October 2008. Available at: http://www.fbi.gov/news/stories/2008/october/darkmarket_102008 (last visited on 22 July 2015).

2.3 The challenge of anonymity

In section 2.2, it was explained how the digital leads of an IP address and an online handle can enable law enforcement officials to gather evidence in a cybercrime investigations. However, cybercrime investigations are seldom as straightforward as explained above. There are three common challenges that law enforcement officials encounter in cybercrime investigations.[46] As mentioned in the introduction of this chapter, these are (1) anonymity, (2) encryption, and (3) jurisdiction.

In this section, the challenge of *anonymity* in cybercrime investigations is further examined. First, the common techniques that cybercriminals use to increase their anonymity by obscuring their IP address are examined in subsections 2.3.1 and 2.3.2. Second, it is explained in subsection 2.3.3 which digital investigative methods law enforcement officials can use to overcome the challenge of anonymity.

2.3.1 Different internet access points

When an individual uses different internet access points (as opposed to typical, household internet connections), it requires (significantly) more effort on the part of law enforcement officials to trace back an IP address.[47] For example, individuals can make use of (a) a WiFi connection of another person, (b) a computer at a cybercafé, and (c) publicly available internet connections (called 'hotspots') at airports, restaurants, or hotels, in order to access the Internet (cf. Bernaards, Monsma & Zinn 2012, p. 61, UNODC 2012, p. 58-60). Law enforcement officials who follow the digital lead of an IP address allocated to these access points will not be directed to the residence or workplace of the suspect, which makes it more difficult to identify a computer user. The example provided below illustrates such a situation.

In 2009, a Dutch minor announced on the online forum '4chan.org' that he would kill his classmates in his Dutch high school.[48] The police likely obtained an IP address from logging information of the post available at 4chan. The IP address was tracked down to a Dutch internet access provider. The subscriber information belonging to the subscription for internet access was subsequently obtained from the provider by use of a data production order. In this case, the suspect used the WiFi connection of his neighbour, thereby leading the law enforcement officials to the residence of his unsuspecting neighbour and her boyfriend, instead of to the suspect's residence. When the law enforcement officials arrived at the suspect's neighbours' house, the neighbours stated that they shared the login credentials

46 These challenges are identified based on literature, the examination of case law, the conducted dossier research, and the conducted interviews.

47 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 11.

48 See Rb. Den Haag, 2 April 2010, ECLI:NL:RBSGR:2010:BM1481.

of their router with a young man living next door to their apartment. This statement provided a new lead to the law enforcement officials and caused them to perform a second search, this time at the residence of the suspect. Eventually, a statement of the suspect himself and a temporary file on his computer containing the actual threat provided the essential evidence for his conviction.[49]

This example illustrates how straightforward it is for cybercriminals to direct law enforcement officials into following the wrong lead. In this case, law enforcement officials were able to identify the suspect. However, this may not have been possible if the suspect had hacked a different WiFi-router to access the Internet that belonged to individuals with no relation to the suspect.[50] As explained above, many other manners exist to access the Internet from a different internet connection. It will depend on the consistency with which an individual makes use of this anonymisation method, the techniques that are used, and the amount of logging information that is available at these internet access points whether an individual can be identified by law enforcement officials.

2.3.2 Anonymising services

There are many anonymising services available on the Internet that make it harder for law enforcement officials to track down suspects based on their IP address (cf. UNODC 2013, p. 143).

The following three services are briefly discussed to illustrate how anonymising services challenge law enforcement officials in gathering evidence: (A) proxy services, (B) VPN services, and (C) Tor.[51]

A Proxy services

Proxy services are services that send network traffic through an intermediary computer; such computers are called 'proxy servers'. A proxy server functions as a gateway. Proxy services strip away the originating IP address. The public IP address of the network connection that a suspect uses is changed to the proxy server's address (cf. Hagy 2007, p. 51-52).[52]

---

49 See Rb. Den Haag, 2 April 2010, ECLI:NL:RBSGR:2010:BM1481, Hof Den Haag, 9 March 2011, ECLI:NL:GHSGR:2011:BP7080 and HR 26 March 2013 ECLI:NL:HR:2013:BY9718.

50 The term 'war driving' is used when referring to the activity of searching for wireless networks to use by using WiFi-enabled equipment such as a laptop from a car (see, e.g., Bryant et al. 2008, p. 113).

51 It is important to note that these three anonymising services are not the only services that provide a degree of anonymity online. For example, Freenet is publicly available software that enables users to anonymously share files and visit websites (see Clarke et al. 2001, and Clarke et al. 2010). In addition, anonymity networks that are still in development – in particular the Invisible Internet Project ('I2P') – may prove to be popular in the near future (cf. Ciancaglini et al. 2013, p. 18).

52 These can be commercially available proxy services, but hacked computers can also act as a gateway for the network traffic of criminals (see Bernaards, Monsma & Zinn 2012, p. 61).

B Virtual Private Network Services

Virtual Private Network services (VPN services) are services that route traffic through an intermediary server, thereby changing the originating (public) IP address of an internet user. In addition to proxy services, VPN services encrypt the internet traffic in transit.[53] The workings of proxy services and VPN services for the situation in which an individual makes use of (broadband) internet connection at this home is illustrated in Figure 2.4.

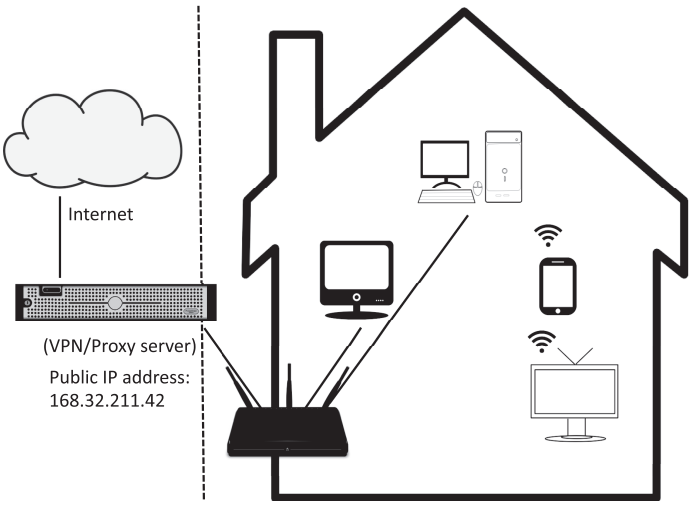

Figure 2.4: Simplified model of an individual that uses of a server of a proxy service or VPN service to access the Internet.

Figure 2.4 illustrates how proxy services and VPN services route traffic through an intermediary server and change the originating (public) IP address of a household internet connection of an internet user to the IP address of a proxy-service provider's server or a VPN-service provider.[54] Proxy-service providers and VPN-service providers provide more anonymity to internet users, because it requires more effort from law enforcement officials to trace an IP address back to the computer user. In essence, intermediary computers are an additional link in the chain.[55]

Law enforcement officials may be still able to trace internet users, depending on the logging information and subscriber data that is available

53 Subsection 2.4.1 under A explains what 'encryption in transit' entails.

54 It depicts a simplified model, because individuals can make use of multiple proxy services or VPN services. Furthermore, individuals can connect to the anonymising services from different places.

55 Internet users can even send network traffic from one proxy to another proxy server or VPN server to create additional links in the chain, e.g., creating a series of obstacles in a criminal investigation. However, the technique may delay network traffic and can create several points of weakness in the ICT infrastructure (cf. Van den Eshof et al. 2002, p. 34-35).

at the anonymity service. Law enforcement officials must examine the log files of the intermediary server of an anonymising service (cf. Casey 2011, p. 693). A logged IP address of a customer may then provide a lead to the originating IP address. Alternatively, law enforcement officials may be able to obtain subscriber data or payment data with data production orders issued to the service, which can be used to directly identify the proxy- or VPN user.

C Tor

Tor is a system designed to anonymise network traffic.[56] The Tor system performs two essential tasks. It *encrypts* network traffic, and it *routes* traffic through relays on its network. Internet traffic goes 'one hop at a time' through relays.[57] Each relay only knows which relay sent the data to it (the last sender) and the next relay through which the data will be routed (first addressee). No individual relay knows the complete path that the network traffic has taken. The Tor system makes sure that traffic analysis techniques cannot establish a link to the connection's source and destination.[58] Using this 'onion routing' technique, Tor makes it possible to use the Internet without revealing the originating public IP address.[59] Note that the Tor system is used by a wide variety of individuals, including (a) people who live in oppressive regimes or activists who are in danger of being prosecuted for their ideas or beliefs, (b) people who want to use the Internet in relative anonymity, and even (c) law enforcement officials who want to use the Internet relatively anonymously.[60] However, the system is also misused by criminals who can (relatively) anonymously trade illegal goods, offer illegal services, and exchange or distribute child pornography (cf. Bernaards, Monsma & Zinn 2012, p. 62, Europol 2015c, p. 19, and Moore & Rid 2016, p. 21).[61]

The workings of the Tor system is illustrated in Figure 2.5.

---

56 Tor is an abbreviation for 'The Onion Routing'.

57 Tor relays are also referred to as 'routers' or 'nodes'.

58 This description of Tor is derived from the article 'What is Tor' from the website of the Electronic Frontier Foundation. Available at: https://www.eff.org/torchallenge/what-is-tor.html (last visited on 6 February 2015) and 'Tor: overview' from the website of the Tor project. Available at: https://www.torproject.org/about/overview.html.en (last visited on 6 February 2015). See Dingledine, Mathewson & Syverson 2004 for a description about the technical workings of Tor.

59 However, some researchers suggest Tor users can be deanonymised. See, e.g., Chakravarty et al. 2014. See also Larry Hardesty, 'Shoring up Tor. Researchers mount successful attacks against popular anonymity network – and show how to prevent them', 28 June 2015. Available at: https://news.mit.edu/2015/tor-vulnerability-0729 (last visited on 27 August 2015).

60 Note that, at the same time, network traffic from Tor can also stand out from regular internet traffic.

61 In the Netherlands, the use of Tor and Tor hidden services by child pornographers became apparent to the public during the prosecution of Robert M. in 2011. See Rb. Amsterdam 23 July 2012, ECLI:NL:RBAMS:2012:BX2325, par 4.4.5 and the press release of the Public Prosecution Service on 31 August 2011, 'Kinderporno op anonieme, diep verborgen websites'. Available at: http://www.om.nl/onderwerpen/verkeer/@156657/kinderporno-anonieme/ (last visited on 1 February 2013).

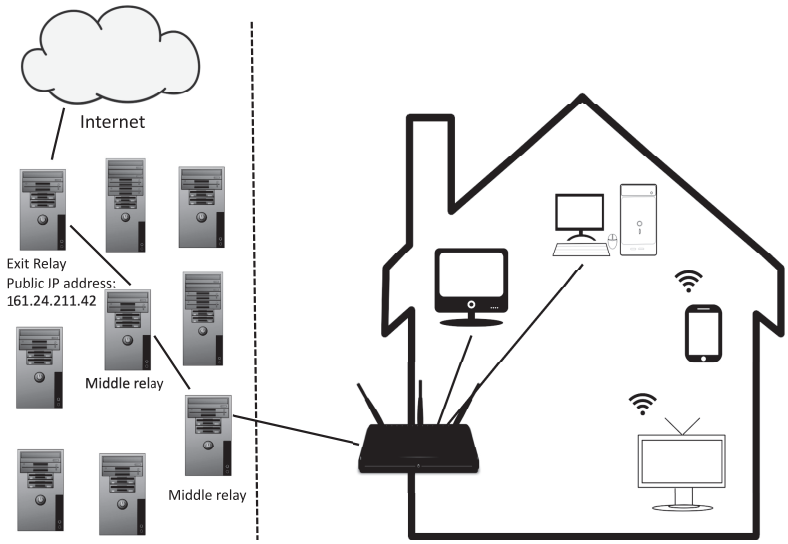

Figure 2.5: Simplified model of how Tor works.

Figure 2.5 illustrates how the Tor system anonymises network traffic by routing internet traffic from one relay to another. Internet traffic that is sent through the Tor system generally passes three relays before it reaches its destination.[62] The first two relays are 'middle relays' that receive traffic and pass it along to another relay. An 'exit relay' is the final relay through which Tor traffic passes before it reaches its destination. Because Tor traffic exits through the exit relay, the IP address of the exit relay is interpreted by others as the source of the traffic.[63] Tor is straightforward to use because it is integrated in a special web browser, which can be downloaded from the website of the Tor project.[64]

Apart from providing the means to hide the originating IP address, the Tor system also allows individuals to access 'hidden services' on the Internet. Hidden services are websites or online services that are only accessible to computers that make use of the Tor system. Tor users can set up a server to publish content on a website, use chat services, and use mail services that are only available to other Tor users.[65] The combination of those websites and services that are publicly accessible and that also hide the IP addresses

62 See https://blog.torproject.org/blog/lifecycle-of-a-new-relay (last visited on 2 February 2015: *"Tor clients generally make three-hop circuits (that is, paths that go through three relays)"*.

63 See 'What is Tor' from the website of the Electronic Frontier Foundation. Available at: https://www.eff.org/torchallenge/what-is-tor.html (last visited on 6 February 2015).

64 See https://www.torproject.org/about/overview.html (last visited on 2 February 2015).

65 See https://www.torproject.org/docs/tor-hidden-service.html.en (last visited on 9 October 2013).

of the servers that run them are referred to as the 'Dark Web'.[66] Since the exact location of these servers is not visible, law enforcement officials cannot use data production orders to gather data from an online service provider. For that reason, at the start of the investigation, other investigative methods must be used to gather evidence.

2.3.3 Overcoming the challenges of anonymity

Law enforcement officials can overcome the challenges of anonymity when investigating cybercrime by using a variety of investigative methods. One such combination of methods is discussed below by detailing the digital investigative methods used in the *Silk Road* investigation. In subsection 2.2.2, it was explained how law enforcement officials can (1) gather personal information about individuals from the Internet, (2) make use of data production orders to gather evidence, and (3) interact with individuals on the Internet using an online handle as a digital lead. Even when individuals make use of anonymising services, an online handle may still provide a powerful lead for law enforcement officials to gather evidence. In addition, law enforcement officials can also gain remote access to computer by use of hacking techniques (called 'hacking as an investigative method' in this study) in order to ascertain the location of the computer.

The *Silk Road* investigation provides a good example of how a combination of investigative methods can enable law enforcement officials to deal with the challenge of anonymity in cybercrime investigations. As explained in subsection 2.1.2, Silk Road was a successful online black market that facilitated the trade in illicit goods and services, primarily drugs. Importantly, Silk Road was a hidden service only accessible through Tor. The webserver of Silk Road and its administrator were therefore difficult to locate for law enforcement officials. The forum administrator used the nickname 'Dread Pirate Roberts' and taunted law enforcement officials by giving interviews to journalists about his successful (and illegal) website.[67] However, the FBI was able to trace 'Dread Pirate Roberts' using the following seven investigative methods:

(1) gathering publicly available online information based on an online handle (i.e., "rossulbricht@gmail.com" that was obtained from an advertisement for Silk Road that Ross Ulbricht (who was identified as Dread Pirate Roberts) posted years before Silk Road became a success);

66 Andy Greenberg, 'Hacker Lexicon: What Is the Dark Web?', *Wired*, 19 November 2014. Available at: http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (last visited on 25 November 2014).

67 See Andy Greenberg, 'An Interview with A Digital Drug Lord: The Silk Road's Dread Pirate Roberts', *Forbes*.com, 13 August 2013. Available at: http://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/ (last visited on 20 November 2015).

(2) issuing data production orders to the following online service providers: Google, WordPress, PayPal, and an online forum;
(3) performing online undercover interactions with Ross Ulbricht on TorChat;
(4) performing pseudo-purchases of drugs on Silk Road;
(5) using identified drug dealers on Silk Road as informants in order to learn more about the website's administrator;
(6) gaining remote access to the server by use of hacking techniques[68]; and
(7) seizing the web server in a data centre[69] after a successful mutual legal assistance request to Iceland and search for evidence stored on the seized webserver of Silk Road.[70]

Eventually, U.S. law enforcement officials traced the suspect Ross Ulbricht to the city of San Francisco. By observing the behaviours of Ross Ulbricht in the physical world and by analysing corresponding activities on the Silk Road's server, the investigators were able to match the times at which Ross Ulbricht turned on his computer and logged onto Silk Road as an administrator.[71] On 1 October 2013, the FBI arrested Ross Ulbricht and seized his laptop in a library in San Francisco.[72] His laptop and the seized Silk Road servers contained the necessary evidence to prosecute Ross Ulbricht for drug trafficking and money laundering. On 5 February 2015, he was found

68 See Andy Greenberg, 'Ross Ulbricht Calls For New Trial, Alleging Feds Hacked Tor', *Wired*, 9 March 2015. Available at: http://www.wired.com/2015/03/ross-ulbricht-calls-new-trial-alleging-feds-hacked-tor/ (last visited on 30 September 2015). U.S. law enforcement authorities never acknowledged they hacked Silk Road's server.

69 The data centre also reportedly kept system logs for six months, which showed all the other computers that had recently communicated with the web server.

70 This can deduced from the court documents involving the Silk Road case and the following articles: Nate Anderson and Cyrus Farivar, 'How the feds took down the Dread Pirate Roberts', *Ars Technica*, 3 October 2013. Available at: http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/, Kim Zetter, 'How the Feds Took Down the Silk Road Drug Wonderland', *Wired*, 18 November 2015. Available at: http://www.wired.com/2013/11/silk-road/, Andy Greenberg, 'Undercover Agent Reveals How He Helped the FBI Trap Silk Road's Ross Ulbricht', *Wired*, 14 January 2015. Available at: http://www.wired.com/2015/01/silk-road-trial-undercover-dhs-fbi-trap-ross-ulbricht/, and Joshuah Bearman, 'Silk Road: The Untold Story', *Wired*, 23 May 2015. Available at: http://www.wired.com/2015/05/silk-road-untold-story/ (last visited on 30 September 2015).

71 Ibid.

72 Note that the arrest was orchestrated in such a way that law enforcement authorities were able to keep the laptop logged into the Silk Road server, while the Silk Road server was secured as evidence in Iceland.

guilty of drug trafficking and money laundering.[73] In May 2015, he was sentenced to life in prison.[74]

The investigative methods used to deal with the challenge of anonymity are for a large part the same as the investigative methods used to gather evidence based on the digital leads of a suspect's online handle(s). Additionally, U.S. law enforcement authorities may have hacked the Silk Road server, which IP address was obscured by the use of Tor, in order to overcome the challenge of anonymity and determine its location.[75] This made it possible to seize the server and subsequently secure its contents in a data centre in Iceland by use of mutual legal assistance.

The Silk Road investigation illustrates how much effort it takes for law enforcement officials to track down suspects who make use of anonymising services. At the same time, the Silk Road investigation illustrates how many individuals find it difficult to consistently use anonymising services and protect their identities. Law enforcement officials use those mistakes to collect the required information to successfully gather evidence and identify suspects. In addition, the use of hacking as an investigative method can be a powerful technique to identify suspects by determining the location and contents of their computer.

2.4 The challenges of encryption

In section 2.2, it was explained that IP addresses and online handles are often the only digital leads at the start of a cybercrime investigation. As explained in section 2.3, the use of different internet access points and anonymising services further challenge law enforcement officials during the first stage of an investigation. Once the communication network which a suspect used or the suspect himself is identified, law enforcement officials commonly face another challenge in cybercrime investigations: the use of *encryption*. The term 'encryption' refers to the process of converting data from its original form ('plain text') into an indecipherable or scrambled form ('cipher text') using a mathematical algorithm.[76] Encryption scrambles data in cipher text,

73 See the press release of the U.S. Department of Justice, 'Ross Ulbricht, The Creator and Owner Of The "Silk Road" Website, Found Guilty In Manhattan Federal Court On All Counts', 5 February 2015. Beschikbaar op: http://www.justice.gov/usao/nys/pressreleases/February15/UlbrichtRossVerdictPR.php (last visited on 30 September 2015).

74 See Sam Thielman, 'Silk Road operator Ross Ulbricht sentenced to life in prison', *The Guardian*, 29 May 2015. Available at: http://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced (last visited on 30 September 2015).

75 See Andy Greenberg, 'Ross Ulbricht Calls For New Trial, Alleging Feds Hacked Tor', *Wired*, 9 March 2015. Available at: http://www.wired.com/2015/03/ross-ulbricht-calls-new-trial-alleging-feds-hacked-tor/ (last visited on 30 September 2015). U.S. law enforcement authorities never acknowledged they hacked Silk Road's server.

76 For purposes of this study, the exact workings of the technologies used for encryption are not relevant and are therefore not analysed in detail. See, e.g., Schneier 2007, for a technical explanation of the workings of encryption.

making it impossible for law enforcement officials to read the contents of data without the key that decrypts data back into plain text.

The use of encryption challenges law enforcement officials in cybercrime investigations in two situations: (1) during the analysis of data in transit that is encrypted (*encryption in transit*) and (2) when law enforcement officials stumble upon encrypted data on computers during a computer search (*encryption in storage*).[77] A 'computer search' is understood in this study as an investigative method in which law enforcement officials search a place in order to seize documents stored on computers for evidence-gathering purposes.

This section examines the technical challenges of encryption. It also identifies the investigative methods that law enforcement officials use to deal with this challenge. The challenges of encryption in transit and encryption in storage are further examined in subsections 2.4.1 and 2.4.2. The digital investigative methods used to overcome the technical challenges of encryption are examined in subsection 2.4.3.

2.4.1 Encryption in transit

Law enforcement authorities in both the Netherlands and the United States warn that their ability to read the contents of intercepted communications is declining. In general, (internet) wiretaps work as follows. Internet wiretaps intercept all incoming and outgoing internet traffic of a network access device, such as ingoing and outgoing internet traffic from a broadband internet router or ingoing and outgoing internet traffic generated by a smartphone.[78]

As a result of encryption in transit, law enforcement officials are often not able to interpret encrypted network traffic that is generated by parties other than internet access providers.[79] This means that the contents of network traffic, such as private messages that are sent over social media services or apps, cannot be read by law enforcement officials (cf. Bellovin et al. 2014a, p. 12). For instance, in 2014, the popular messaging service WhatsApp implemented 'end-to-end encryption'. Subsequently, law enforcement officials were no longer able to read intercepted information from WhatsApp.

---

77 Authors such as Wiemans (2004, p. 168-169), Byrant et al. (2008, p. 98), and Koops (2012, p. 16) previously made the distinction between encryption in transit and encryption in storage.

78 See Odinot et al. 2012 and Oerlemans 2012 for a more extensive analysis. With regard to wiretapping internet traffic from a smartphones, it is likely that a more unique identifying number is used, such as an IMEI-number or a mobile telephone number.

79 Internet access providers have to decrypt data that these 'public telecommunication service- or network providers' encrypt themselves. Many online service providers are not considered as 'public telecommunication service- or network providers' or reside on foreign territory, outside the reach of law enforcement authorities (see Oerlemans 2012, p. 26).

There is not even a decryption key available at WhatsApp that may be obtained by a legal order, because the keys are stored at the end users' computers.[80] Apple's popular iMessage service reportedly also enables end-to-end encryption and hinders the wiretapping efforts of law enforcement authorities.[81]

Law enforcement authorities view their declining ability to intercept electronic communications in plain text as a major obstacle, because wiretaps have historically provided law enforcement officials with useful evidence in criminal investigations. Stated differently, law enforcement authorities argue that they are '*going dark*', because their practical ability to intercept electronic communications is declining.[82] Below, (A) developments in the use of encryption in transit and (B) other developments that make internet wiretapping less effective are examined.

A Developments in the use of encryption of data in transit

Three developments regarding the use of encryption of data in transit can be distinguished. They challenge law enforcement officials in criminal investigations in particular and are mentioned below.

The first development is the increase of default encryption implemented by popular online communication service providers. For example, Microsoft's webmail Hotmail (now Outlook mail), all services provided by Google, the microblog service Twitter, and the social media service Facebook are all encrypted by default.[83] Intercepted communications from these

80 See Ellen Nakashima, 'WhatsApp, most popular instant-messaging platform, to encrypt data for millions', *The Washington Post*, 19 November 2014. Available at: http://www.washingtonpost.com/world/national-security/whatsapp-worlds-most-popular-instant-messaging-platform-to-encrypt-data-for-millions/2014/11/18/b8475b2e-6ee0-11e4-ad12-3734c461eab6_story.html (last visited 27 November 2014).

81 Dan Goodin, 'Apple's iMessage crypto stymies federal eavesdropping of drug suspect', *Ars Technica*, 4 April 2013. Available at: http://arstechnica.com/tech-policy/2013/04/apples-imessage-crypto-stymies-federal-eavesdropping-of-drug-suspect/ (last visited 29 December 2014). However, see also the (partly technical) analysis of Nicolas Weaver in the article of Paul Rosenzweig, 'iPhones, the FBI, and Going Dark', 4 August 2015. Available at: https://www.lawfareblog.com/iphones-fbi-and-going-dark (last visited 18 August 2015). Weaver points out that, for example, traffic data is still available for analysis by law enforcement authorities. See subsection 2.2.2 under B with regard to the term 'traffic data'.

82 See the Statement of Valerie Caproni: "*In the ever-changing world of modern communication technologies, however, the FBI and other government agencies are facing a potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications*". See also Ellen Nakashima, 'Proliferation of new online communications services poses hurdles for law enforcement', *The Washington Post*, 25 July 2014. Available at: http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html (last visited 25 July 2014).

83 Interestingly, the switch to encrypted traffic by these services (except Gmail, because Google's webmail service applied encryption by default before) occurred in only two years' time between 2011 and 2013.

online services are likely no longer readable for law enforcement officials when an internet wiretap is used to gather evidence (unless the results of the communications are publicly accessible on the Internet) (cf. Swire 2012, p. 202-203).

The second development regards the increased use of anonymising services that encrypt network data by default. Internet traffic that is routed through VPNs and Tor is encrypted by default, making the data unreadable for law enforcement officials without the keys to decrypt the data (cf. Koops et al. 2005, p. 61, and Bernaards, Monsma & Zinn 2012, p. 62).[84] In 2015, Europol stated: *"the use of simple proxies and VPNs has continued to increase in the past 12 months and is now the norm amongst cybercriminals"* (Europol 2015b, p. 51). Europol also noted that *"the adoption of Tor as an anonymising solution has seen the greatest growth in the past 12 months, with half of EU Member States noting an increase in its use of obfuscation of criminal activity"* (Europol 2015b, p. 51).

The third development regards the increased use of a manual encryption of electronic communications by individuals. Internet users can manually encrypt specific electronic communication services by using programs such as 'Pretty Good Privacy' (PGP) to encrypt the contents of e-mail messages (cf. Singleton 2008, p. 294-295).[85] Europol noted an increase of the use of encrypted messages with PGP by cybercriminals in 2015 (Europol 2015b, p. 50).

B Other developments in internet wiretapping

It is important to point out that the use of encryption techniques is only one of four reasons why the practical ability of law enforcement officials to intercept electronic communications is declining. The other three reasons for the limited usefulness of internet wiretapping as an investigative method are: (1) legal and geographical limits, (2) the fragmented use of internet connections, and (3) the amount of traffic and diversity in Internet protocols. The other three reasons are briefly considered below.

(1) Wiretapping is legally and geographically limited to the investigating State's territory. Law enforcement authorities can only enforce wiretapping obligations on communication service providers that reside within the investigating State's territory. Law enforcement officials typically wiretap all traffic that is generated by a broadband internet connection from an internet access provider or network traffic generated by smartphones (see Smits 2006, p. 77 and Oerlemans 2012, p. 22). There is no connection available to wiretap when an individual

84 See also the *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 9.

85 However, there are news articles that suggest that Dutch law enforcement authorities (with the aid of the National Forensic Institute) are able to decrypt encrypted messages by PGP on certain mobile telephones. See, e.g., Jan Meeus, 'De crimineel sms't, de politie kijkt mee', *NRC Handelsblad*, 20 June 2016.

does not make use of a telecommunication provider within the investigating States territory. For instance, internet wiretapping by Dutch law enforcement authorities can only take place within the territorial borders of the Netherlands. American online service providers cannot be forced to wiretap information for Dutch law enforcement authorities.

(2) When using an internet wiretap, only network traffic from a broadband internet connection or network traffic generated by smartphones can be intercepted. This means that in many cases only part of the network traffic that an individual makes use of during the day is intercepted. The reason is that people also often use WiFi connections and 'hotspots' with WiFi connections offered by restaurants, public transportation companies, and hotels to access the Internet (cf. Koops et al. 2005, p. 61). As a result, law enforcement authorities will often obtain only a fragmented picture of the electronic communications of a targeted individual within a specific time frame (cf. Koops et al. 2005, p. 63, Oerlemans 2012, p. 30-31 and Bellovin et al. 2013, p. 63-64).[86]

(3) The amount and variety of information that is intercepted in a wiretap has strongly increased over the last decade. For law enforcement officials, it is a challenge to interpret the large amounts of internet network traffic generated by many different applications, which often use different communications protocols (cf. Koops et al. 2005, p. 60, Diffie & Landau 2007, p. 55, and Odinot et al. 2012, p. 158).

Considering the above-mentioned developments in internet wiretapping, it is unsurprising that a Dutch evaluation report on wiretapping explicitly states that Dutch law enforcement officials experience the limits imposed by encryption of data in transit as a major challenge in criminal investigations (see Odinot et al. 2012, p. 129).

However, instead of arguing that law enforcement officials are losing wiretapping as an important instrument in criminal investigations, one can also argue that technology provides law enforcement officials with more powerful means of gathering evidence in criminal investigations than in the pre-internet era (cf. Swire and Ahmad 2012). For example, Swire and Ahmad argue that law enforcement are currently experiencing 'a golden age of surveillance' due to (1) the amount of information that is publicly available online, (2) the ability to intercept traffic data (including location data) despite the challenge of encryption in transit, and (3) the ability to acquire data with data production orders from online service providers (cf. Swire and Ahmad 2012, p. 463-474).

86 The Dutch legislator explicitly mentions the wide variety in internet connections as a challenge to fully intercept electronic communications of an individual (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 11).

The changes in the investigative powers of law enforcement authorities caused by technological developments indeed seem to lead to a new balance of power. However, when taking together the technological developments that have taken place in the past five years, news articles regarding the use of anonymising techniques and encryption techniques by criminals, the available literature on the topic, and conducted interviews with experts, it appears that the power of law enforcement authorities to intercept communications has declined considerably. This development has a large impact on criminal investigations conducted by Dutch law enforcement authorities. Dutch law enforcement authorities heavily rely on wiretapping as an investigative method in criminal investigations involving serious crime (see Odinot et al. 2012, p. 104-105). Law enforcement authorities must therefore seek alternatives for obtaining the evidence required to successfully prosecute cybercrimes.

2.4.2 Encryption in storage

Law enforcement authorities also view the encryption of data in storage as a growing challenge in criminal investigations.[87] The use of encryption to protect data in storage changes readable (plain text) data on a computer into cipher text. The use of encryption in storage makes the information unreadable for law enforcement officials when the decryption key is unavailable.

Whether law enforcement officials are capable of decrypting data depends on many different factors. For example, the strength of the password used to protect the key is a factor. Depending on the circumstances of the case and encryption techniques that are utilised, law enforcement officials may be able to recover sufficiently incriminating evidence from unencrypted areas of storage media (cf. Casey et al. 2011, p. 129). Law enforcement officials may also be able to exploit the sloppiness of an individual who uses encryption to protect his data (see Koops 2012b, p. 23-24). A telling example of this is the Russian espionage case of Anna Chapman and Mikhail Semenko in the United States. In this case, the FBI managed to overcome the challenge of encryption in storage by recovering pieces of paper containing the necessary passphrases to decrypt the data (see Casey et al. 2011, p. 131). A different strategy is to prevent individuals from turning on an encryption measure. Law enforcement officials will meticulously plan seizures of computers ahead of time in order to seize a suspect's computer while it is still running, thereby giving the suspect no chance to turn on an

87 See, e.g., Faber et al. 2010, p. 118 and p. 300, Brenner 2011, p. 82, Koops et al. 2012, p. 21 and 44-46, and Mevis, Verbaan & Salverda 2016, p. 58. See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 8.

encryption feature (Casey 2011, p. 131).[88] Of course, law enforcement officials can also request that a suspect voluntarily give up his password to decrypt information.

Despite these workarounds to handling the challenge of encryption in storage, it is clear that encryption poses a challenge in cybercrime investigations. Europol stated in 2015 that: *"More than three-quarters of cybercrime investigations in the EU encountered the use of some form of encryption to protect data and/or frustrate forensic analysis of seized media"* (Europol 2015b, p. 50).[89] Two reasons why encryption in storage has become a major challenge in cybercrime investigations are that encryption techniques have become easy to use and that encryption is a standard feature in many computers and operation systems.

In particular, the use of (A) full disk encryption and (B) the encryption of files stored in the cloud pose significant challenges for law enforcement officials in criminal investigations. These encryption techniques are further examined below.

A Full disk encryption

Full disk encryption is a security measure in which a storage medium, such as hard disc, in a computer is fully encrypted. Implementing full disk encryption as a security measure is not difficult. Freely available encryption software, such as TrueCrypt, can fully encrypt a storage medium. Full disk encryption is also offered as a standard security option on computers (cf. Chatterjee 2011, p. 276). For law enforcement authorities, it is reportedly not possible to 'break' modern encryption within a reasonable timeframe (cf. Europol 2015b, p. 69).

In 2014, the director of the FBI first publicly declared how standard encryption measures on iPhones and Android phones also hamper law enforcement officials.[90] Apple and Google reportedly encrypt their phones "*so thoroughly (...) that the company is unable to unlock iPhones or iPads for*

88 For example, in the Silk Road case, the FBI meticulously planned the arrest of Ross Ulbricht to make sure his computer remained turned on after seizure to prevent encryption and perform live forensics. See Joshuah Bearman, 'Silk Road: The Untold Story', *Wired*, 23 May 2015. Available at: http://www.wired.com/2015/05/silk-road-untold-story/ (last visited 30 September 2015).

89 Mevis, Verbaan & Salverda (2016, p. 58) state that over half of the respondents in their interviews indicate that encryption in storage 'regularly' imposes a challenge in their criminal investigations (with regard to all types of crimes in the Netherlands).

90 Technically, the standard encryption measures on iPhones work differently than full disk encryption. However, they are comparable and the security measure poses law enforcement authorities the same problem.

police".[91] The standard device encryption on modern iPhones is an ongoing problem for law enforcement authorities at the time of writing (October 2016).[92] Full disk encryption on a computer and standard device encryption may therefore leave law enforcement authorities unable to analyse data on a seized computer if they do not obtain the encryption key in order to decrypt the data on the computer (cf. Casey et al. 2011).[93]

B Encryption of files stored in the cloud

Cloud computing enables people to log in to a web portal and make use of electronic communication services and online storage services.[94] Law enforcement officials seeking information that is made available through these web portals cannot obtain the information by seizing a computer and analysing the information stored on it. Instead, the information is sent back and forth by the online service providers and is processed on the servers in data centres of online service providers. Law enforcement officials can possibly intercept the data in transit. However, as already stated above, the challenge of encryption in transit makes it impossible under certain circumstances for law enforcement officials to read the contents of network traffic.[95]

---

91 Craig Timberg and Greg Miller, 'FBI blasts Apple, Google for locking police out of phones', The Washington Post, 25 September 2014. Available at: http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html (last visited on 25 September 2014). However, note that the user must utilise a strong password and not the 4-digit passcode as a security measure. It is straightforward to crack a 4-digit passcode. See the analysis of Nicolas Weaver in the article of Paul Rosenzweig, 'iPhones, the FBI, and Going Dark', 4 August 2015. Available at: https://www.lawfareblog.com/iphones-fbi-and-going-dark (last visited 18 August 2015).

92 Matt Burgess, 'Tim Cook: Apple won't weaken encryption to meet FBI demands', Wired, 12 February 2016. Available at: http://www.wired.co.uk/news/archive/2016-02/17/tim-cook-apple-encryption-iphone-san-bernardino (last visited on 18 April 2016).

93 In certain circumstances and on certain computers, law enforcement officials can perform 'live forensics'. In the process of live forensics, volatile information is captured from physical memory on a computer system (cf. Adelstein 2006, p. 64). That volatile information may include an encryption key, which can be used to decrypt the data stored on a computer system. Therefore, live forensics may be a solution for full disk encryption or partial encryption of disks (cf. Casey 2011 et al. p. 132, Bryant et al. 2008, p. 105-110, and Koops et al. 2012b, p. 46).

94 Cloud computing has been defined as *"a model for enabling convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Mell & Grance 2009). This is the definition used by the U.S. National Institute of Standards and Technology (NIST). For this study only cloud computing techniques relating to Software as a Service (SaaS) are considered. SaaS is software provided by a third party provider running on a cloud infrastructure. Available on demand and accessible from various devices through an interface, such as a web browser or App. Examples of SaaS are web based email services, online word processing tools and web content delivery services.

95 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 10.

The manual encryption in storage of files 'in the cloud' appears to be a major challenge for law enforcement authorities. In this case, a user encrypts files before uploading them to the servers of cloud providers (cf. Colarusso 2011, p. 92-93). These files are unreadable by law enforcement officials, even when they collect the files from third party providers through data production orders.

2.4.3 Overcoming the challenges of encryption

The challenges of encryption in transit and encryption in storage make it more difficult for law enforcement officials to read the content of intercepted network traffic and analyse data after the seizure of a computer.

However, law enforcement officials can use digital investigative methods to overcome these challenges and gather evidence. The investigative methods of (A) data production orders that are issued to online service providers and (B) hacking as an investigative method, can be used to overcome the challenges of encryption in transit and encryption in storage. These digital investigative methods are further examined below.

A Data production orders issued to online service providers

As explained in subsection 2.2.2 under B, data production orders enable law enforcement officials to obtain data from online service providers. Thus, companies that provide online storage services can also be forced to hand over decrypted data to law enforcement officials when they are issued with a data production order. Online service providers are often able to decrypt data themselves (1) for advertisement purposes, (2) in case a customer forgets his password, and (3) for security purposes and for law enforcement purposes (cf. Soghoian 2010, p. 52 and 70-71).[96]

Therefore, even though an individual may have enabled full disk encryption on a computer, law enforcement officials may be able to collect a copy of that data from an online service provider. For example, if an iPhone is encrypted and law enforcement seeks to obtain information stored on it, they may be able to obtain the information by issuing a data production order to Apple in order to collect a backup copy of the contents of an

96 For example, Apple can decrypt information from their customers and law enforcement authorities. See Apple iCloud's Terms and Conditions: *"You acknowledge and agree that Apple may, without liability to you, access, use, preserve and/or disclose your Account information and Content to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate, if legally required to do so or if Apple has a good faith belief that such access, use, disclosure, or preservation is reasonably necessary to: (a) comply with legal process or request; (b)* (...) *or (d) protect the rights, property or safety of Apple, its users, a third party, or the public as required or permitted by law."* Available at http://www.apple.com/legal/icloud/en/terms.html (last visited 20 October 2016).

iPhone.[97] Swire predicts that the challenges of encryption will drive law enforcement authorities to issue more data production orders to online service providers (cf. Swire 2012).[98]

B Performing hacking as an investigative method

Law enforcement officials can also gain remote access to computers to overcome the challenges of encryption in transit and encryption in storage. In this study, the investigative activity in which law enforcement officials can gain remote access to computers is called 'performing hacking as an investigative method'. Hacking as an investigative method can be best described as an umbrella term, which encompasses different investigative methods that have in common that law enforcement officials remotely obtain access to a computer system (cf. Oerlemans 2011, p. 891).

Hacking is distinguished in this study as an investigative method which appears in the following three forms: (B.1) network searches, (B.2) remote searches, and (B.3) the use of policeware (cf. Oerlemans 2011 and Conings & Oerlemans 2013). These three types of hacking are further examined below.

B.1 Network searches

A network search is an investigative method that takes place during a search at a particular place (in the physical world). During a network search, law enforcement officials gain remote access to an interconnected computer that is connected to a computer that has been previously seized (for instance, during a search of a residence). As part of a network search, law enforcement officials can then examine an external hard drive or media player that is part of the same (internal) network.

A network search can enable law enforcement officials to deal with the challenge of encryption in storage by accessing remotely stored information through an interconnecting computer. A network search is considered as a type of hacking as an investigative method, because law enforcement officials can gain remote access to a computer system (of which the suspect is not necessarily aware). For instance, remotely stored information may be accessible through an online account that can be accessed with obtained log-

97 Law enforcement officials may be able to obtain data that is backed-up by Apple's iCloud service. See C. Foresman, 'Apple holds the master decryption key when it comes to iCloud security, privacy', *Ars Technica* 2012. Available at: http://arstechnica.com/apple/2012/04/apple-holds-the-master-key-when-it-comes-to-icloud-security-privacy/. See also Nicolas Weaver in the article of Paul Rosenzweig, 'iPhones, the FBI, and Going Dark', 4 August 2015. Available at: https://www.lawfareblog.com/iphones-fbi-and-going-dark (last visited 18 August 2015).

98 However, note that, law enforcement officials may not be able to acquire the data within an acceptable time frame due to unacceptable delays in mutual legal assistance procedures (cf. NIST 2014, p. 7). See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 9. See section 2.5 for further analysis with regard to the challenge of jurisdiction cybercrime investigations.

in credentials.[99] Using a network search, law enforcement officials can gain access to online accounts of individuals through a running seized computer (cf. Conings & Oerlemans 2013).[100] The prevalence of 'apps' on smartphones with accompanying login credentials make it possible for law enforcement officials to use those credentials and collect evidence that can be accessed through programs located on a seized computer that is connected to the Internet.

B.2 Remote searches

The investigative method of a remote search refers to an evidence-gathering activity in which law enforcement officials remotely access a computer and search the data that is stored on it (cf. Brenner 2012).

Remote searches may enable law enforcement officials to deal with the challenge of encryption in storage in criminal investigations. By using the proper investigative method, law enforcement officials can gain remote access to a computer that a suspect uses. After remote access is obtained, law enforcement officials can take screen shots of the computer, write down a report of the evidence-gathering activities, or even copy relevant data for evidence-gathering purposes (cf. Oerlemans 2011, p. 892). In this manner, law enforcement officials can avoid seizing a computer during a search and can analyse a computer before the data stored on a computer is encrypted.

B.3 The use of policeware

Law enforcement officials can overcome the challenge of encryption in transit by intercepting communications of an individual 'at the source', i.e., the computer itself, before encryption in transit is enabled for communications (cf. Abate 2011, p. 124).[101] This can be made possible by using 'computer monitoring software', which is called 'policeware' in this study.[102] To use policeware, law enforcement officials must remotely gain access to a computer and install the software. The software may enable law enforcement officials to log the suspect's keystrokes. Thereafter, the officials can remotely

99 Law enforcement officials can obtain login credentials from programs at the seized computer or from cookies to access certain web services. Login credentials can also be obtained through informants or voluntarily provided by a suspect.

100 See also the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53. Available at: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/herziening-van-het-wetboek-van-strafvordering (last visited February 2016). The Dutch legislator indicates that Dutch law enforcement officials can log in to a server of Gmail or Dropbox to access e-mails and documents stored 'in the cloud'.

101 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 10.

102 Jacobs (2012) first used the term 'policeware' in literature.

turn on the computer's microphone.[103] Subsequently, the recorded data is sent to law enforcement officials. The use of policeware enables law enforcement officials to intercept communications in criminal investigations.[104]

Law enforcement officials can also overcome the challenge of encryption in storage using policeware. With the ability to intercept keystrokes of a computer user, law enforcement officials can collect individuals' passwords and login credentials (cf. Fox 2007, p. 828). Passwords that are logged by a keylogging functionality of policeware can be used to decrypt a hard disc or files of an individual (cf. Oerlemans 2011, p. 905-907). Policeware can also create a 'back door' to computers for law enforcement authorities to remotely access a computer. As noted above (under B.2), law enforcement officials can then look at the computer screen through the eyes of a suspect by taking screenshots. After remote access has been obtained to a computer of a suspect, law enforcement officials can copy data that they deem relevant to an investigation. For this reason, the use of policeware can take place prior and in conjunction with the investigative method of a remote search.

Finally, it should be noted here that policeware can also be used to overcome the challenge of anonymity in cybercrime investigations. Once law enforcement officials gained remote access to a computer and installed the software, the software can be directed to send law enforcement officials the originating (public) IP address of the computer and other identification information.[105] The FBI reportedly makes use of policeware with specifically these functionalities.[106] In the last decade, the use of policeware enabled

103 Commercially available software for law enforcement authorities reportedly have these capabilities. See, e.g., Morgan Marquis-Boire, 'From Bahrain With Love: FinFisher's Spy Kit Exposed?', *Citizen Lab*, 25 July 2012. Available at: https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/ (last visited on 10 July 2014), Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, 'Mapping Hacking Team's "Untraceable" Spyware', *Citizen Lab*, 17 February 2014.

104 Commercial policeware vendors reportedly advertise this kind of software with the following description: "*A stealth, spyware-based system for attacking, infecting and monitoring computers and smartphones. Full intelligence on target users even for encrypted communications (Skype, PGP, secure web mail, etc.)*" (Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, 'Mapping Hacking Team's "Untraceable" Spyware', *Citizen Lab*, 17 February 2014 with reference to http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf (last visited on 10 July 2014).

105 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 19-20.

106 Reportedly, software is available that provides U.S. law enforcement with the following information: (a) the IP address of the computer, (b) MAC address, (c) a list of open TCP and UDP ports, (d) a list of running programs, (e) operation system information, (f) default internet browser and version, (g) registered user of the operation system, (h) currently logged in user, and (i) last visited URL. See Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', *Wired*, 18 July 2007. Available at: http://archive.wired.com/politics/law/news/2007/07/fbi_spyware (last visited on 30 December 2014). The information is obtained through data access requests to U.S. governmental agencies.

them to identify individuals that made anonymous bomb threats through webmail in the United States.[107]

2.5 The challenge of jurisdiction

From section 2.2 to section 2.4, it has been explained how law enforcement officials can gather evidence in cybercrime investigations, even when the technical challenges of anonymity and encryption arise. However, even though law enforcement officials may be technically able to gather the evidence in a cybercrime investigation, they can still face legal challenges. In this section, the legal challenge of jurisdiction is further examined. It also identifies the approach that law enforcement officials use to overcome this challenge in cybercrime investigations.

This section examines the legal challenge of jurisdiction. The examination is started by providing a brief description of the concept of enforcement jurisdiction in subsection 2.5.1. Then, the mechanism of mutual legal assistance to obtain evidence located on foreign territory is examined in subsection 2.5.2. Subsequently, the limits of mutual legal assistance as a mechanism for extraterritorial evidence-gathering activities in cybercrime investigations are addressed in subsection 2.5.3. Finally, the way law enforcement officials overcome the challenge of jurisdiction is examined in subsection 2.5.4.

2.5.1 Enforcement jurisdiction

The term 'jurisdiction' describes the limits of the legal competence of a State or a different regulatory authority to make, apply, and enforce rules of conduct upon persons (see Lowe 2006, p. 335 in: Evans 2006). In European criminal law, the 'jurisdiction' of a State is split into (1) the capacity to make and apply law (*jurisdiction to prescribe*) and (2) the capacity to ensure compliance with such laws through executive, administrative, police or other non-judicial action (*jurisdiction to enforce)*.[108] This study focuses on the jurisdiction to enforce.

---

107 See, e.g., Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', *Wired*, 18 July 2007. Available at: http://archive.wired.com/politics/law/news/2007/07/fbi_spyware and Kevin Poulson, 'Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years', *Wired*, 16 April 2009. Available at: http://www.wired.com/2009/04/fbi-spyware-pro/ (last visited on 30 December 2014).

108 See, e.g., Mann 1984, O'Keefe 2004, p. 737-738, Lowe in: Evans (ed.) 2003, p. 329, and Shaw 2008, p, 645-646. In U.S. criminal law, a third category of 'adjudicative jurisdiction' is distinguished, which refers to a sovereign's authority to have its courts determine whether a particular law was violated (see Restatement (Third) of Foreign Relations Laws of the United States par 401(a)-(c) (1987)). However in practice, courts decide whether a person is guilty of criminal behaviour by applying its national criminal laws and thus prescriptive jurisdiction and adjudicative jurisdiction collapse into one (cf. Akehurst 1974, p. 179, O'Keefe 2004, p. 737-738, and Kohl 2007, p. 16).

The jurisdiction to enforce is territorially limited. The common view is that States can investigate crimes on their territory on their own terms, as part as the execution of their sovereign rights. This strict territorial limitation of the jurisdiction to enforce has been explicitly made clear by the Permanent Court of Justice in 1927.[109] In the landmark case of *Lotus v. Turkey*, the Permanent Court of Justice stated that:

"The first and foremost restriction imposed by international law upon a State is that – failing existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention".[110]

Thus, law enforcement officials cannot mount an investigation on foreign territory without ad hoc permission or a treaty.[111] Crawford (2012, p. 479) aptly describes the territorial restriction of enforcement jurisdiction as follows:

"Persons may not be arrested, a summons may not be served, police or tax investigations may not be mounted, order for production of documents may not be executed, except under the terms of a treaty or other consent given."

When law enforcement officials unilaterally gather evidence on foreign territory without the permission of the affected State and without a treaty basis that authorises the evidence-gathering activity, their behaviour infringes upon the following three principles of international law: (1) sovereignty, (2) equality of States, and (3) the principle of non-intervention (cf. Shaw 2008, p. 645). These three principles are briefly discussed below.

(1) *Sovereignty*. Sovereignty refers to a State's privilege to exercising power over its territory (cf. Stigall 2012, p. 328).[112] As part of its territorial sovereignty, States regulate the use of governmental power in relation to investigative methods that are utilised over individuals on their own territory.[113] The manner in which a State regulates the evidence-gathering activities of law enforcement officials within its territorial borders falls within the exercise of its sovereign rights (cf. UNODC 2013, p. 184). Therefore, when foreign law enforcement authorities wield their power over citizens of another State, it infringes on the sovereignty of the State in which those citizens live.

109 PCIJ, SS Lotus (France v. Turkey), 1927, *PCIJ Reports*, Series A, No. 10.
110 PCIJ, SS Lotus (France v. Turkey), 1927, *PCIJ Reports*, Series A, No. 10, p. 18-19.
111 See also, e.g., Reijntjes, Mos & Sjöcrona, p. 257 in: Van Sliedregt, Sjöcrona & Orie 2008.
112 Referring to Cassese 2005, p. 49.
113 However, note that fundamental human rights and international treaties restrict the exercise State power over individuals on its territory (cf. Gill 2013, p. 221 in: Ziolkowlski 2013).

(2) *Equality of States*. The principle of the legal equality of States implies that, formally speaking, all members of the international community are on the same footing (see Cassese 2005, p. 52). Whatever their size or power, States have a duty to not intervene in the internal affairs of other States.
(3) *Principle of non-intervention.* The duty not to intervene in the internal affairs of other States is called the principle of non-intervention (cf. Shaw 2008, p. 212).[114] Together with the principle of sovereign equality, the principle of non-intervention is designed to ensure that each State respects the fundamental prerogatives of other members of the community (cf. Cassese 2005, p. 53).

These three principles are considered as the 'cornerstones of international law' (cf. Ryngaert 2007, p. 40). Ultimately, these principles are essential to maintaining a reasonably stable system of competing States (cf. Shaw 2008, p. 213). As Shaw explains: *"setting limits on the powers of States vis-à-vis other states contributes to some extent to a degree of stability within the legal order"* (Shaw 2008, p. 213). States that gather evidence on the territory of another State, without permission or consent derived from a treaty, can enter into conflict. The reason is that these extraterritorial evidence-gathering activities can be perceived as an infringement of the territorial sovereignty of the other State. The extraterritorial enforcement of jurisdiction is therefore only possible with permission of the affected State or based on a treaty (see Mann 1964, p. 44-49).

As a consequence of the territorial sovereignty of a State, States have (a) local criminal laws that specify which behaviours are considered as 'cybercrimes', (b) local authorities who investigate cybercrimes under local laws that stipulate the scope of the instruments that can be used to investigate crime, and (c) local authorities that prosecute cybercrime in local courts.

In cybercrime investigations, law enforcement officials are often required to gather evidence on foreign territory and prosecute foreign individuals (cf. UNODC 2013, p. 119). Therefore, it should be observed that the investigation and prosecution of cybercrime take place *locally* and are limited by the physical borders of a State, whereas cybercrimes themselves are often *cross-border* in nature (cf. Brenner & Schwerha IV 2002, p. 395).

Of course, States have developed a mechanism to collect evidence on foreign territory without infringing on the territorial sovereignty of the State in which the evidence is located. That mechanism is known as mutual legal assistance and is further analysed in the subsection below.

114 The principle of non-intervention in international law is also reflected in the U.N. General Assembly's Declaration on Principles of International Law Concerning Friendly Relations and Cooperation, which states: *"No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State"* (general assembly of 24 October 1970, 25th session, A/RES/25/2625) (cf. Stigall 2012, p. 336). See also art. 2(7) of the Charter of the United Nations.

2.5.2 Mutual legal assistance

Mutual legal assistance is the formal procedure by which states request and obtain evidence on foreign territory.[115] States can agree on the conditions under which evidence can be gathered on their territory upon request by local law enforcement authorities or even unilaterally by foreign law enforcement officials under supervision of local law enforcement authorities. The conditions in which mutual legal assistance is provided to other law enforcement authorities can be agreed upon in treaties.

Below, the Convention on Cybercrime (under A) and the Treaty of Lisbon (under B) are briefly examined in order to illustrate how mutual legal assistance mechanisms work in the context of cybercrime investigations.

A Convention on Cybercrime

The Convention on Cybercrime is the most important multilateral treaty in cross-border cybercrime investigations.[116] The convention is particularly important for the following three reasons.

(1) *Harmonisation of criminal substantive law with regard to cybercrime*. Harmonisation of criminal substantive law facilitates mutual legal assistance, because States will criminalise harmful behaviours in a similar manner. In that case, it is easier for States to agree on mutual legal assistance to gather evidence from other States and to extradite individuals.

(2) *The obligation to regulate certain investigative powers in a domestic legal framework*. The regulation of investigative powers is important, because they provide the practical tools for law enforcement authorities to investigate cybercrimes.

115 Notably, mutual legal assistance also entails (1) the exchange of information ('intelligence') between law enforcement authorities, (2) the transfer of criminal proceedings, and (3) the extradition of suspects. This study focuses on the evidence-gathering activities in criminal investigation by law enforcement authorities using investigative methods in cybercrime investigations. As a consequence, informal cooperation between law enforcement authorities is also not considered. Law enforcement officials in the Netherlands do not have the authority to gather evidence with investigative methods and exchange evidence with their foreign counterparts without permission of the formal authority (usually a public prosecutor), even when law enforcement authorities have the authority to gather evidence themselves. Although some authors question whether public prosecutors are able to practically supervise the exchange of evidence under informal constellations between law enforcement authorities, it is clear that – in theory -only a model of formal mutual legal assistance for evidence gathering on foreign territory applies in the Netherlands (see Reijntjes, Mos & Sjöcrona, p. 263 in: Van Sliedregt, Sjöcrona & Orie 2008 and Vander Beken 1999, p. 341). See more generally with regard to police cooperation, the exchange of intelligence, and the international criminal law framework, e.g., Bassiouni 2008, p. 19-21.

116 See for an extensive analysis of the Convention on Cybercrime, e.g., Kaspersen, p. 156-172 and 175-180 in: Koops 2007 and Oerlemans 2016, in: Verrest and Paridaens 2016.

(3) *The creation of a system for swift international cooperation*. The Convention on Cybercrime obliges member states to create a contact point to ensure the provision of immediate mutual legal assistance for cybercrime investigations.[117] The contact point must be available twenty-four hours a day, seven days a week. The contact point ensures that the assigned law enforcement authority within a member state is able to coordinate mutual legal assistance proceedings with other law enforcement authorities. The idea is to make mutual legal assistance procedures in cybercrime investigations more efficient.

However, two States that are crucial to cybercrime investigations, Russia and China, did not ratify the Convention on Cybercrime. Therefore, these States (1) may have regulated cybercrimes in a completely different manner, (2) have not necessarily implemented the mentioned investigative powers in their domestic legal frameworks, and (3) do not have a contact point that is obliged to cooperate with foreign law enforcement authorities that ratified the convention. This may frustrate international cybercrime investigations.

In addition to the Convention on Cybercrime, many other multilateral treaties aim to harmonise criminal substantive laws with regard to cybercrimes.[118] However, those other treaties do not harmonise investigative methods for evidence-gathering purposes.[119] So far, efforts to provide for a global (UN) treaty to harmonise cybercrimes and provide for a more effective mechanism to gather evidence in criminal investigations involving cybercrime have failed.[120] Apparently, the majority of States are unwilling to give up part of their territorial sovereignty to regulate the ways in which evidence can be collected in cybercrime cases.

117 See art. 35 of the Convention on Cybercrime.

118 See UNODC 2013, p. 63-76 for an overview of treaties with regard to cybercrime. Five regional or international clusters that developed treaties can be identified which are the (1) Council of Europe or the European Union, (2) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (3) intergovernmental African organizations, (4) the League of Arab States, and (5) the United Nations (UNODC 2013, p. 63).

119 See extensively, e.g., UNODC 2013, p. 63-71.

120 See Chief Judge Stein Schjølberg, 'Report of the Chairman of HLEG to ITU Secretary-General Dr. Hamadoun I. Touré', *ITU Global Cybersecurity Agenda (GCA)*, High-Level Experts Group (HLEG) 2008, p. 6-9. Available at: http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf (last visited 25 February 2015). See also Stein Schjølberg and Solange Ghernaouti-Helie, 'A Global Treaty on Cybersecurity and Cybercrime', 2nd ed., 2011.

B Treaty of Lisbon

The Treaty of Lisbon is of great significance to evidence-gathering activities within the European Union.[121] Since the ratification of the Treaty of Lisbon in 2007, the legislative authorities of the European Union are authorised to impose binding rules on evidence-gathering activities in criminal matters (cf. Summers et al. 2014, p. 46).[122]

However, at this time (October 2016), there is (1) no EU law enforcement authority, (2) no EU prosecution authority, and (3) no EU court with jurisdiction to try individuals who violate EU criminal law (cf. Summers et al. 2014, p. 272). Currently, there are 28 different national criminal procedural codes in the European Union that regulate evidence-gathering activities by law enforcement officials in criminal investigations in their own manner.[123] As a result, in international criminal investigations, the criminal procedural laws of the individual member states dictate how evidence must be obtained from each territory, unless specific treaty provisions apply. Not surprisingly, strict formalities and lengthy mutual legal assistance procedures often plague cooperation between States in the EU (cf. Cryer et al. 2010, p. 88).

The EU instrument of 'mutual recognition' aims to change the traditional principle that the local laws of the 'requested State' stipulate under which conditions evidence is gathered ('*locus regit actum*'). Mutual recognition means that States within the EU must recognise each other's judicial systems and must immediately execute mutual legal assistance requests under the criminal procedural laws of the issuing (EU Member) State with a minimum of formality and exceptions (cf. Bantekas 2007). Most notably, the 'European Investigation Order' is a mutual legal assistance instrument that ensures that an 'issuing State' can collect evidence with co-operation of the 'executing State' under the formalities and procedures expressly indicated

121 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon on 13 December 2007, entered into force on 1 December 2009, OJ C306.

122 Criminal law and criminal procedural law can be harmonised upon the basis of art. 82 of the Treaty on the Functioning of the European Union (TFEU). The EU has the explicit competence to harmonise computer crime between Member States in art. 83(1) TFEU (see Summers et al. 2014, p. 233). However, note that a legal procedure was created in art. 83(3) TFEU called the 'emergency break procedure', which allows member states to protest against legislation that would affect fundamental aspects of their criminal justice system (see for a more extensive analysis, e.g., Klip 2012, p. 36 and Summers et al. 2014, p. 46-78). The United Kingdom, Ireland and Denmark made reservations to the applicable EU treaties on mutual legal assistance in criminal investigations and do not take part in all treaties (see Mitsilegas 2009, p. 53-56).

123 Following the referendum in the United Kingdom on 24 June 2016, a majority of the British people voted to leave the EU. It is possible the United Kingdom will soon leave the EU. See also Jennifer Rankin, Jon Henley, Philip Oltermann, and Helena Smith, 'EU leaders call for UK to leave as soon as possible', *The Guardian*, 24 June 2016. Available at: http://www.theguardian.com/politics/2016/jun/24/europe-plunged-crisis-britain-votes-leave-eu-european-union (last visited on 26 June 2016).

by the issuing State.[124] Overall, the European Investigation Order has the potential for a more efficient means to gather evidence in criminal investigations.[125]

However, even when the European Investigation Order is used, local law enforcement officials within a particular State gather the evidence.[126] Thus, the law enforcement officials of the investigating State still depend on the cooperation of law enforcement officials in the requested State. Currently, there is no broader vision in the European Union to fight crime under harmonised criminal procedural rules (cf. Klip 2012, p. 473). Summers et al. (2014, p. 283) observe: *"there is a clear and overt resistance among Member States to further communitarisation"*.[127] This becomes apparent in the manner the EU seeks to combat cybercrime. The EU Directive 2013/40/EU concerning 'attacks against information systems' harmonised criminal substantive law in relation to target cybercrimes and established mandatory minimum penalties for these crimes.[128] However, the directive does not harmonise criminal procedural law, which may facilitate evidence-gathering activities in cybercrime investigations. Harmonisation of criminal procedural law within the EU to combat cybercrime is also not expected in the near future.

---

124 See the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal Matters, (OJ L 130/1). The European Investigation Orders also applies to 'computer related offences' (see Appendix D of the Directive). Not all cross-border evidence-gathering activities fall under the Directive. Recital 24 notes that additional rules are necessary for (a) the temporary transfer of persons held in custody, (b) hearing by video or telephone conference, (c) obtaining of information related to bank accounts or banking transactions, (d) controlled deliveries, and (e) covert investigations. The European Investigation Order also does not apply to the investigative methods of wiretapping and the data production orders issued to electronic communication service providers (cf. Van Daele 2012, p. 219-220). Moreover, there are grounds for States to refuse the European Investigation Order. The most important exceptions are stipulated in art. 9(2), art. 9(5) and art. 11 of Directive 2014/41/EU.

125 At the same time, the European Investigation Order is strongly criticised by legal scholars. See for, example, Ruggeri (in: Ruggeri 2014, p. 3) who argues that there is no proper balance between the efficiency of prosecution and the protection of human rights of the individuals involved. See also: Raad voor de Rechtspraak, 'Wetsvoorstel Europees onderzoeksbevel biedt onvoldoende bescherming', 5 November 2015. Available at: https://www.rechtspraak.nl/Organisatie/Raad-Voor-De-Rechtspraak/Nieuws/Pages/Wetsvoorstel-Europees-onderzoeksbevel-biedt-onvoldoende-bescherming.aspx (last visited 9 November 2015).

126 Note that even when law enforcement authorities of the issuing State are present on the territory of the other State, the authorities: *"shall be bound by the law of the executing State during the execution of the EIO. They shall not have any law enforcement powers in the territory of the executing State, unless the execution of such powers in the territory of the executing State is in accordance with the law of the executing State and to the extent agreed between the issuing authority and the executing authority."* (art. 9(5)).

127 Referring to Mitsilegas 2009.

128 See EU Directive 2013/40/EU about 'attacks against information systems' (2013/40/EU (L218/8) of 14 August 2013. The Directive also forces member states to respond to mutual legal assistance requests within eight hours and to indicate whether the request will be answered and the form and estimated time of the answer. See for a more extensive analysis of EU criminal law and cybercrime, e.g., Summers et al. 2014, p. 231-254.

2.5.3 Limits of mutual legal assistance

Mutual legal assistance, as a mechanism to obtain evidence on foreign territory, has two important limitations. The first limitation is that mutual legal assistance is only available insofar States are able to agree upon the conditions for extraterritorial evidence gathering. Law enforcement officials are completely dependent on the willingness of local law enforcement authorities to cooperate when no treaty can be negotiated. The second limitation is that mutual legal assistance procedures can be burdensome for law enforcement authorities, especially in cybercrime investigations (cf. Prins 2012, p. 49). In other words, mutual legal assistance procedures can take too much time for law enforcement officials.

Mutual legal assistance procedures can become significantly more burdensome when suspects make use of anonymising services to change the visible IP address. This enhanced jurisdictional challenge is illustrated in Figure 2.6.

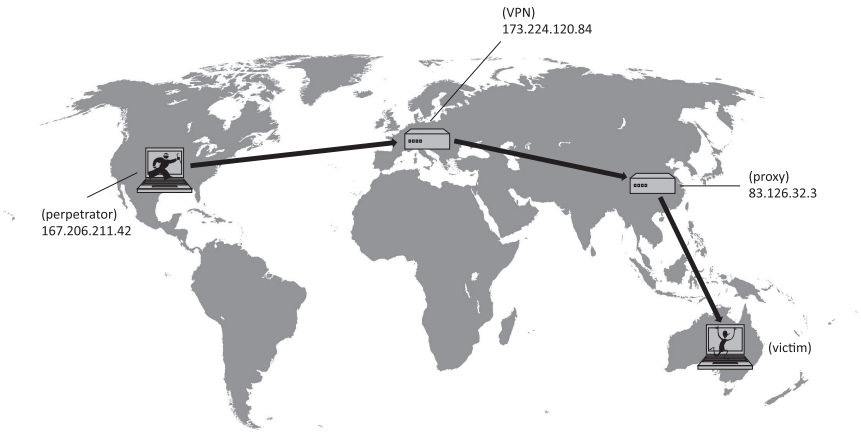

Figure 2.6: Illustration of the global nature of cybercrime and the jurisdiction challenge in cybercrime investigations.

Figure 2.6 illustrates a criminal in the United States using a VPN server in Germany and a proxy server in China to obscure his IP address and commit a crime in Australia. In that case, law enforcement officials in Australia have to use mutual legal assistance procedures to collect evidence from a proxy-service providers and VPN-service providers in order to follow up on the digital lead of an IP address. Following Figure 2.6, in order trace back the suspect, law enforcement officials require subscriber data from (1) a proxy provider in China, (2) a VPN provider in Germany, and (3) an internet access provider in the United States. Thus, evidence must be obtained from online service providers in each successive jurisdiction through which the communication passes (cf. Sussmann 1999, p. 468). As explained in subsection 2.3.2, a proxy service and VPN service may provide an additional link in the chain

to trace back the address of an internet user. Tracing back the originating IP address of a computer therefore requires a considerable amount of time.

To conclude, gathering of evidence in cross-border cybercrime investigations through the mutual legal assistance model can be burdensome (even between Member States of the European Union). When cybercriminals make use of anonymising services, it can be even more difficult to obtain evidence by use of mutual legal assistance procedures. In situations where the requested state is unwilling or unable to afford mutual legal assistance, law enforcement officials are left empty handed (cf. Stigall 2013, p. 23). To be direct: current mutual legal assistance mechanisms seem to be unable to meet the investigative and prosecutorial challenges of cybercrime investigations (cf. UNODC 2013, p. 214 and Koops & Goodwin 2014, p. 41).[129]

2.5.4 Overcoming the challenge of jurisdiction

Law enforcement officials can overcome the challenge of jurisdiction in cybercrime investigation by gathering evidence across State borders. The Internet can facilitate evidence-gathering activities that may take place on foreign territory, while investigators are still within the territorial borders of the investigating State (cf. Siemerink 2000c, p. 240). Thus, digital investigative methods can be applied within the territorial borders of the investigating State and produce effects outside the investigating State territorial borders at the same time. For instance, law enforcement officials can chat with an individual on foreign territory to gather evidence in a domestic criminal investigation.

Practically, no mutual legal assistance is required to gather the evidence. Therefore, cross-border unilateral evidence-gathering activities that are facilitated by the Internet can be regarded as a manner of overcoming the challenge of jurisdiction in cybercrime investigations. Law enforcement officials may be inclined to succumb to unilateral action when there are no mutual legal assistance treaties in place or the data cannot be acquired within a reasonable time frame (cf. NIST 2014, p. 7). The following Dutch case is illustrative for this situation. In 2008, a Dutch public prosecutor instructed a law enforcement official to log in to a Hotmail account, using login credentials that were provided by an informant.[130] The public prosecutor was of the opinion that it would take too much time to obtain the documents from Microsoft (offering the webmail service 'Hotmail').[131] In the view of the public prosecutor, the circumstances of the case required immediate action, because law enforcement officials expected to find the details about a large delivery of cocaine in the port of Rotterdam in the Netherlands in

129 See also See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 49.

130 Rb. Rotterdam, 26 March 2010, ECLI:NL:RBROT:2010:BM2520 and Hof Den Haag, 27 April 2011, ECLI:NL:GHSGR:2011:BR6836.

131 The webmail service 'Hotmail' has been recently rebranded by Microsoft as 'Outlook mail'.

the Hotmail account. After the law enforcement officials gained access to the incriminating e-mails in the Hotmail account, the information in those e-mails indeed led to the seizure of cocaine stored in a ship in the port of Rotterdam.[132]

However, theoretically, law enforcement officials can infringe on the territorial sovereignty of a State when their investigative activities produce extraterritorial effects. As extensively explained in subsection 2.5.1, extraterritorial investigations of law enforcement officials without permission or consent derived from a treaty basis with the affected State are not allowed by international law.

New regime in international law?

To solve this problem, one option is to create a completely new legal regime in international law in order to allow the application of extraterritorial investigative techniques by use of digital investigative methods. In the early 1990s, certain legal scholars submitted that "cyberspace" is a distinct "place", which is not subject to the traditional notions in law.[133] In addition, more recently, legal scholars suggested that a new legal regime in international law should be applicable to cyberspace. Inspired by the special legal regime for outer space or the high seas, some scholars suggested that a similar legal regime should apply to cyberspace.[134] Other scholars suggested that cyberspace should be viewed as a 'global commons' that should be regulated by global treaties.[135]

These suggestions for an alternative legal regime in international law for cyberspace have not taken root (cf. Pirker 2013, p. 195 in: Ziolkowski 2013 and Koops & Goodwin 2014, p. 67). States have consistently applied their territorially based rules to behaviours of individuals that are facilitated by the Internet, refusing to treat the Internet as a 'separate place' with different rules (cf. Kohl 2007, p. 11, Pirker 2013, p. 194 in: Ziolkowski 2013 and Koops & Goodwin 2014, p. 21). In other words, the legal world is still very much

132 See the facts of the case described in Rb. Rotterdam, 26 March 2010, ECLI:NL:RBROT:2010:BM2520. Interestingly, there are no other published judgements available in the Netherlands, which indicate that law enforcement authorities gained remote access to the contents of webmail services. Perhaps this case turned up the surface, because the public prosecutor in question specifically requested the judge to decide whether the investigative method was a legitimate investigative power.

133 See most notably, Johnson and Post, whom argued that the Internet undermined the feasibility – and legitimacy – of laws based on geographical boundaries (Johnson & Post 1996, p. 1378). This notion has been nicely described by John Perry Barlow in the first paragraph of his 'Declaration of Cyberspace', written on 8 February 1996: "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.*" Available at https://projects.eff.org/~barlow/Declaration-Final.html (last visited 1 March 2015).

134 See, e.g., Franzese 2009, Stahl 2011 and Hildebrandt 2013.

135 See, e.g., Lukasik 2000. See Koops & Goodwin (2014, p. 67-77) for an overview and analysis of alternative legal regimes of international law for 'cyberspace'.

divided into territorial borders of sovereign States (see, e.g., Van Staden & Vollaard 2002, p. 183 in: Kreijen et al. 2002 and Stigall 2013, p. 9).

To conclude, investigative activities that take place on the Internet are subjected to the normal rules of international law on the exercise of jurisdiction (cf. Pirker 2013, p. 196 in: Ziolkowski 2013). Thus, the investigative activities of law enforcement officials in cybercrime investigations are restricted by the territorial limitation of enforcement power. At the same time, this study holds a realistic view of the application of investigative methods to cybercrime investigations. States continue to apply their rules to behaviours that take place on the Internet, but this does not negate the fact that the Internet is a borderless medium that does not take territorial borders into account.

Disparity of the legally divided world and online investigations

Currently, there is a disparity between the *theory* of a world that is legally divided by the territorial borders of sovereign States and the *reality* of an interconnected world in which law enforcement officials can virtually cross State borders.[136] In 1998, the Dutch legislature observed that the possibility of cross-border unilateral online investigations may be in conflict with the territorial sovereignty of other States.[137] According to the Dutch legislature, further research was required into how to deal with this legal issue.[138] However, very little research has been performed with regard to the question of the applicability and desirable territorial limits of these online investigations.[139]

The cross-border unilateral application of digital investigative methods and the tension that this approach poses to the principle of the territorial limitation of enforcement jurisdiction is further examined in chapter 9.

2.6 Chapter conclusion

The aim of this chapter is to determine which digital investigative methods are commonly used in cybercrime investigations (RQ 1). To answer RQ 1, a three-step approach was taken. In step one, the object of the criminal investigation, cybercrime, was examined. In step two, the two digital leads that law enforcement officials often follow in cybercrime investigations and the

136 See also Koops & Goodwin 2014, p. 78 who observe: *"In our research, we are struck by the lack of understanding with cyber-investigation experts of basic principles and developments of international law as well as by the lack of understanding with international law experts of basic principles and developments of cyber-investigation"*.

137 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1997/98, 25 880, no. 1, p. 81

138 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1999/2000, 25 880, no. 10, p. 24.

139 With the notable exceptions of the article of Siemerink in 2000(c) and the report of Koops & Goodwin in 2014.

accompanying evidence-gathering activities were examined. In step three, the three challenges in cybercrime investigations and the digital investigative methods used to overcome these challenges were analysed.

Step one was addressed in section 2.1 by providing a typology of cybercrime. Three examples of target cybercrimes and three examples of tool cybercrimes were provided to illustrate how computers and the Internet facilitate cybercrime. This knowledge was required to understand how the type of crime, in this case *cybercrime*, influences criminal investigations. In brief, the analysis has shown that criminals can take advantage of computers and the Internet to commit crimes relatively anonymously across State borders. They can also reach many computer users as potential victims.

Step two was addressed in section 2.2 by explaining the investigative activities that law enforcement officials take based on the two digital leads of (1) IP addresses and (2) online handles. The analysis showed that law enforcement officials use the following digital investigative methods to gather evidence based on these two leads: (a) gathering publicly available online information, (b) issuing data production orders to online service providers, and (c) applying online undercover investigative methods.

Step three was addressed in three parts in the sections 2.3 to 2.5. Three challenges in cybercrime investigations were identified as (1) anonymity, (2) encryption, and (3) jurisdiction. The analysis showed that the technical challenge of anonymity can be overcome by using the same investigative methods as those based on the digital leads from online handles. The analysis with regard to the technical challenges of encryption showed that law enforcement officials can overcome this challenge by using (a) data production orders that are issued to online service providers and (b) hacking as an investigative method. The analysis with regard to legal challenge of jurisdiction has shown that mutual legal assistance – a mechanism for gathering evidence that is located on foreign territory – is often too burdensome for cybercrime investigations. Practically speaking, law enforcement officials can also gather evidence unilaterally across State borders. In that case, law enforcement officials of the investigating State gather evidence that may be located on foreign territory. These evidence-gathering activities are in tension with the principle of the territorial limitation of enforcement jurisdiction.

These three steps lead to the conclusion that the following digital investigative methods are commonly used – and applied across State borders – in cybercrime investigations:

(1) gathering of publicly available online information;
(2) issuing data production orders to online service providers;
(3) applying online undercover investigative methods; and
(4) performing hacking as an investigative method.

3 Normative requirements for investigative methods

The aim of this chapter is to answer the second research question (RQ 2): *Which normative requirements can be derived from art. 8 ECHR for the regulation of investigative methods?* The chapter is brief, as it intends only to provide a general overview of the normative requirements that apply for the regulation of investigative methods in domestic law.

To answer RQ 2, the relation between the right to privacy as defined in art. 8 ECHR and the regulation of investigative methods is analysed. Art. 8 ECHR provides for an overarching legal framework by imposing certain normative requirements for the regulation of investigative methods in the domestic laws of contracting States to the ECHR. These normative requirements are thus relevant for all contracting States to the ECHR.

The structure of this chapter is as follows. Section 3.1 analyses the scope of protection of the right to privacy as articulated in art. 8 ECHR. In section 3.2, the text of this article is examined to determine which conditions apply to legitimise privacy interferences caused by the use of investigative methods by law enforcement officials. As announced in chapter 1, although all aspects of art. 8 ECHR will be discussed, the focus of this study is on the requirements in this provision that determine how investigative methods should be *regulated* by law. The emphasis of the examination will thus lie in the examination of those aspects of art. 8 ECHR. This examination then serves as the basis for deriving the normative requirements for the regulation of investigative methods. Again, as explained in chapter 1, art. 8 ECHR and the accompanying case law of the ECtHR currently are not specifically oriented on 'the digital world', with case law on the relationship between treaty provisions and digital interferences being sparse. The normative framework examined in this chapter is thus general and mainly derived from case law concerning non-digital interferences. The requirements for digital interferences will be extrapolated from this framework and, in chapter 4, applied to digital investigations methods. The regulations in Dutch law upon which digital investigative methods are based in practice will be tested against these requirements in chapters 5 to 8. In section 3.3, the concept of 'the dynamic interpretation of the ECHR' that the ECtHR uses to interpret the convention rights is examined. In this light, the importance that art. 8 ECHR may have for the regulation of digital investigative methods in the (near) future is also considered. Finally, section 3.4 presents a summary of the chapter's findings.

3.1 The scope of protection under art. 8 ECHR

Art. 8 ECHR reads as follows:

"*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Based on the text above, the right to privacy protects the following four aspects: (1) the right to respect for private life, (2) the right to respect for family life, (3) the right to respect for the home, and (4) the right to respect for correspondence. In a criminal investigation, the use of classical investigative methods, such as a house search and the interception of correspondence, interfere specifically with the right to respect for a *home* and *correspondence*. More novel investigative methods, such as the use of closed-circuit television cameras (hereinafter CCTV) or GPS beacons for surveillance purposes, interfere with the – more broadly formulated – *right to respect for private life* of art. 8(1) ECHR.[1] In its case law, the ECtHR has expanded the protection of art. 8 ECHR to encompass new investigative methods (cf. Ölçer 2008, p. 255).

The ECtHR deliberately does not provide an exhaustive definition of the right to respect for private life.[2] This allows the ECtHR to recognize and include new (types of) privacy interferences and interpret the right to privacy dynamically as a fundamental right. The case law shows the flexibility of art. 8 ECHR in light of both the development and use of new technologies in criminal investigations.[3]

1 See, e.g., ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 57, ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 43 and ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, § 64: "*Article 8 is not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world. Private life may even include activities of a professional or business nature (…) There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"* (...)"

2 In the case of *Niemietz v. Germany* the ECtHR stated that it *"does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life"* (ECtHR 26 December 1992, *Niemietz v. Germany*, appl. no. 13710/88, § 29).

3 See further section 3.3 with regard to the dynamic interpretation of the ECHR.

Negative and positive obligations

The ECtHR interprets art. 8 ECHR (and other convention rights) in such a way that both 'negative' and 'positive' obligations follow from the right to privacy. Negative obligations require a State to refrain from interfering with convention rights, unless they can be legitimatised under the conditions stipulated in those convention rights. Positive obligations require a State to take the steps necessary to adopt reasonable and suitable measures to protect the rights of the individual (cf. Akandji-Kombe 2007, p. 7). The text of art. 8 ECHR itself suggests that only negative obligations follow from that article, as it states "there shall be no interference by a public authority with the right to privacy", except when the conditions stipulated in art. 8(2) ECHR are met. Positive obligations based on art. 8 ECHR are therefore an implicit construction of a convention right by the ECtHR itself. In the context of (digital) investigative methods, case law with regard to positive obligations that follow from art. 8 ECHR is scarce.

However, the case of *K.U. v. Finland* is a noteworthy exception. In this case, the ECtHR determined that Finland had a positive obligation to implement legislation that makes it possible to obtain identifiable data, i.e., subscriber data, from online service providers for the prevention of disorder and crime.[4] The case of *K.U. v. Finland* involved a 12-year-old child whose picture and personal information was abused by an individual: the suspect used the child's information to place advertisements on the Internet stating that the minor wanted to explore sexual relationships. Paedophiles subsequently harassed the child. Finnish law enforcement officials started an investigation but were unable to obtain subscriber data from the online forum provider about the user who had placed the advertisement.[5] The ECtHR did not accept this situation and decided that States have a positive obligation to enable law enforcement authorities to obtain data from online service providers in order to identify internet users based on their IP address. The ECtHR stated that:

"*Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such a guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.*"[6]

4 ECtHR 2 December 2008, *K.U. v. Finland*, appl. no. 2872/02.

5 The reason why law enforcement officials were unable to obtain subscriber data was that there was no investigative power available in Finnish law that provided law enforcement authorities with the authority to obtain subscriber data.

6 ECtHR 2 December 2008, *K.U. v. Finland*, appl. no. 2872/02, § 49.

In other words, the right to privacy under art. 8 ECHR can also lead to an obligation to protect individuals from privacy interferences by other individuals. For the purposes of this study, positive obligations such as those determined in *K.U. v. Finland* serve to confirm the necessity of the proper regulation of digital investigative methods in the current reality. At this time, computers and the Internet play a prominent role in society and creates a platform for crime, against which citizens must be protected. With the duty to protect in this positive sense, States must ensure that domestic law enforcement has the ability to apply the digital investigative methods necessary to an investigation. The negative duty to interfere only legitimately, brings with it that the necessary methods must be regulated in a manner compliant with art. 8 ECHR.

Negative and positive obligations can further be relevant in the context of another treaty concept invoked by the ECtHR, namely extraterritorial obligations. Based on these obligations, States can be held to treaty compliance even outside their own sovereign territory. Case law concerning obligations of States to respect treaty requirements in their actions abroad has been substantially developed.[7] In theory, it could be envisaged that a duty may exist for member States to protect their citizens against interferences on their own territory – through the Internet – by foreign agents acting from other jurisdictions, in or outside of Europe. Case law in this sense is, however, unknown to the author, so that it cannot be contended that such obligations can currently be based on the ECHR. This is not to say however that obligations such as these do not flow forth from rule of law requirements, such as those requiring legal certainty. Such obligations can be important in the context of the cross-border unilateral application of digital investigative methods that can interfere with the right to privacy of individuals who are located in a different State. This topic is revisited in chapter 9.

7 See, e.g., ECtHR 12 December 2001, *Banković and Others v. Belgium and Others*, appl. no. 52207/99, ECtHR 16 November 2004, *Issa and Others v. Turkey*, appl. no. 31821/96, ECtHR 12 May 2005, *Öcalan v. Turkey*, appl. no. 46221/99, ECtHR 7 July 2011, *Al-Skeini and others v. The United Kingdom*, appl. no. 55721/07, and ECtHR 27 October 2011, *Stojkovic v. Belgium and France*, *EHRC* 2012/23, m.nt. F.P. Ölçer. It is important to note that discussion exist about the extent to which the ECHR applies extraterritorially. See with regard to this discussion, e.g., De Schutter 2006 and King 2009. However, when digital investigative methods are applied by law enforcement officials from the investigating State, it is in my view clear that the ECHR protects the citizens that are affected by the application. It is irrelevant whether those individuals live on the territory of the investigating State or outside the territory of the investigating State. See Milanovic (2015, p. 97-99) for a similar reasoning in the context of (digital) mass surveillance measures.

3.2 Conditions to legitimise privacy interferences

When investigative methods are applied, an interference with the right to privacy may take place.[8] Art. 8(2) ECHR states that such a privacy interference is legitimate when the following three conditions are met: a legitimate aim is available (see 3.2.1), the interference is 'in accordance with the law' (see 3.2.2), and the interference is 'necessary in a democratic society' (see 3.2.3). In subsection 3.2.4, the relationship between the gravity of the privacy interference and the quality of the law is further discussed by explaining the workings of the 'scale of gravity' for privacy interferences.

Although all three conditions can be pertinent to the evaluation of compliance of national law with art. 8 ECHR, the second condition being 'in accordance with the law', is particularly important for the regulation of investigative methods *in abstracto*. As this last aspect is the focus of the study, the second requirement will be examined thoroughly. In contrast, the other two conditions for legitimising privacy interferences under art. 8 ECHR, namely having a legitimate aim and being necessary in a democratic society, do not play a central role in this research. It is not to say that they are never relevant. The condition that privacy interferences must be necessary in a democratic society can be important in particular, as it requires a balance between privacy interferences and legitimate aims. The test whether an interference is necessary in a democratic society is generally conducted *in concreto*, based on the facts of a specific case, rather than when regulating the investigative methods *in abstracto* in legislation. However, for particularly intrusive investigative methods, such as those that involve mass surveillance or hacking as an investigative method, the 'necessary in a democratic society' condition may play an important role.[9] Zuiderveen Borgesius and Arnbak (2015) rightfully pose the question whether it is desirable that all privacy interferences can be legitimised by 'proceduralising' them in legalisation. Legislatures should also take the scope of an investigative method into account and decide at which point an investigative method can no longer be considered 'necessary in a democratic society'. The three conditions for legitimising privacy interferences are further examined below.

---

8 It is important to realise that not necessarily all investigative methods interfere with the right to privacy as defined in art. 8 ECHR. For example, the ECtHR has considered that no interference with the privacy takes place when law enforcement officials take a photo of an individual at a public demonstration. See ECtHR 25 September 2001, *P.G. and J.H. v The United Kingdom*, appl. no. 44787/98, § 58 with reference to ECtHR 31 January 1995, *Friedl v. Austria*, § 51-52.

9 It is possible the ECtHR will decide on the legitimacy of these mass surveillance measures in one of the following cases: ECtHR 4 September 2013, *Big Brother Watch and Others v. The United Kingdom,* appl. no. 58170/13, ECtHR 11 September 2014, *Bureau of Investigative Journalism and Alice Ross v. The United Kingdom,* appl. no. 62322/14, and ECtHR 20 May 2015, *Human Rights Organisations v. The United Kingdom*, appl. no. 24960/15. In the same sense, the (total) absence of a legitimate aim behind a legal provision of an investigative method may also offend the requirements of art. 8 ECHR.

3.2.1 A legitimate aim is available

The first condition is that *a legitimate aim* must be available when investigative methods are used that interfere with the right to privacy. In the context of criminal investigations, the legitimate is often 'the prevention of disorder or crime' (cf. Krabbe, p. 160 in: Harteveld 2004). In practice, States rarely encounter problems in arguing and demonstrating that a 'legitimate aim is pursued' when investigative methods are used that interfere with the right to privacy in criminal investigations. Instead, the ECtHR often focuses on the other two conditions, i.e., whether the interferences are 'in accordance with the law' and 'necessary in a democratic society', to determine whether a particular privacy interference is legitimate (cf. Gerards 2011, p. 133).

3.2.2 In accordance with the law

The second condition is that interferences with the right to privacy that are caused by the use of investigative methods are '*in accordance with the law*'. The ECtHR uses a broad interpretation of the term 'law'. According to the ECtHR, the law concerns both (a) written law, including published guidelines for the application of investigative methods, and (b) unwritten law, such as settled case law.[10]

In its case law, the ECtHR has stipulated that the regulation of investigative methods must fulfil the following three requirements in order to be considered 'in accordance with the law': (1) *accessibility*, (2) *foreseeability*, and (3) a certain *quality of the law*.[11] In this study, these three requirements are thus considered as the *normative requirements* for the regulation of investigative methods based on art. 8 ECHR. They are further examined below.

A Accessibility

The first requirement for the regulation of investigative methods is 'accessibility', which means that the law gives an 'adequate indication' concerning which regulations apply for using investigative methods in a given case (cf. Greer 1997, p. 10).[12] The applicable statutory law, case law, or guidelines for

10 See, e.g., ECtHR 24 April 1990, *Kruslin v. France*, appl. no. 11801/85, §28 and *Huvig v. France*, app. no 11105/84, § 29 and ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, §66. See also ECtHR 26 April 1979, *Sunday Times v. The United Kingdom*, appl. no. 6538/74, § 49, and ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 27.

11 It should be noted that in case law, the ECtHR does not always strictly divide these three requirements in this order. In certain cases, the ECtHR only tests the foreseeability of the law, which is then considered as part of the required quality of the law. See, e.g., ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 60.

12 See, e.g., ECtHR 26 April 1979, *Sunday Times v. The United Kingdom*, appl. no. 6538/74, § 49, ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 26, ECtHR 3 April 2007, *Copland v. The United Kingdom*, appl. no. 62617/00, § 46, and ECtHR 10 March 2009, *Bykov v. Russia*, appl. no. 4378/02, § 76.

a certain investigative method must be publicly available. Secret guidelines set by law enforcement authorities in relation to the application of investigative methods are thus not considered as accessible law.[13]

B Foreseeability

The second requirement for the regulation of investigative methods is 'foreseeability', which means that the law must indicate with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which the investigative method is exercised (cf. Gerards 2011, p. 128). In addition to written law and unwritten (case) law, relevant preparatory work for the legislation and publicly available guidelines are also taken into consideration in order to determine whether the law is sufficiently foreseeable in light of art. 8 ECHR (see Ölçer 2008, p. 292).[14]

The ECtHR has explained multiple times that it considers the 'essential object of protection' of art. 8 ECHR to "*protect the individual against arbitrary action by the public authorities*".[15] This is an important statement in relation to the foreseeability requirement in art. 8(2) ECHR. The foreseeability requirement stipulates that both (1) the scope of the power conferred upon the competent authorities and (2) the manner in which the investigative method is exercised must be clear to the individuals involved. If these two conditions are not met, individuals are subjected to an arbitrary interference by governmental authorities in their private lives. The foreseeability requirement in art. 8 ECHR thus offers *legal certainty* to the individuals who are involved in criminal investigations (cf. Krabbe, p. 165 in: Harteveld 2004). Legal certainty about the conditions and the manner in which investigative methods are applied is in turn a key element of the rule of law.[16] By imposing legal constraints on governmental officials in their activities, an uncontrolled and arbitrary application of coercion by the government is avoided. That is not to say that legality is the only requirement of the rule of law.[17]

13 See, e.g., ECtHR 23 September 1998, *Petra v. Romania*, appl. no. 27273/95, § 38.

14 See, e.g., ECtHR 24 March 1988, *Olsson v. Sweden*, appl. no. 10465/83, §62 and ECtHR 24 May 1988, *Müller and Others v. Switzerland*, appl. no. 10737/84, §29.

15 See, e.g., ECtHR 26 December 1992, *Niemietz v. Germany*, appl. no. 13710/88, § 31 and ECtHR 27 October 1994, *Kroon and Others v. The Netherlands*, appl. no. 18535/91, § 31.

16 See also the Council of Europe Commissioner for Human Rights, 'The rule of law on the Internet and in the wider digital world', Issue Paper of 8 December 2014, p. 8.

17 Tamanaha (2004) distinguishes a formal definition of the rule of law and a substantive definition of the rule of law. In the formal definition, governmental officials and citizens are bound by and act consistent with the law. In the substantive definition, fundamental rights, democracy, and concepts such as 'human dignity' are also taken into account. After all, the fact that governmental officials are bound by the law, does not say anything about the content of the law. See for an extensive analysis, e.g., Tamanha 2004, p. 91-101.

C Quality of the law

The third requirement for the regulation of investigative methods is a sufficient 'quality of the law'. The ECtHR has clarified in its case law that investigative methods that interfere with fundamental rights cannot be expressed in a legal framework 'in terms of an unfettered power' that is conferred on law enforcement authorities.[18] The ECtHR can subsequently specify (1) the level of detail of the regulations and (2) the minimum procedural safeguards that must be implemented in the domestic legal frameworks of contracting States to the ECHR (cf. Gerards 2011, p. 129). These detailed regulations and procedural safeguards in domestic law aim to counterbalance the risk of abuse of power by the government (cf. Krabbe, p. 167 in: Harteveld 2004).[19]

3.2.3 Necessary in a democratic society

As a third condition for legitimising privacy interferences, art. 8(2) ECHR requires that the legitimate aim being pursued by a government when applying investigative methods that interfere with the right to privacy of citizens must be '*necessary in democratic society*'. To determine whether this condition is met, the ECtHR tests whether the inference with the right to privacy (1) corresponds to a 'pressing social need' and (2) is 'proportionate to the legitimate aim pursued'.[20] In doing so, the ECtHR essentially examines whether a fair balance is met between (1) the interference with the right to privacy of the involved individual on the one hand and (2) the necessity to use the privacy infringing investigative method on the other hand (see Gerards 2011, p. 140).

The ECtHR applies the test whether application of the investigation is 'necessary in a democratic society' *in concreto*. That means that the ECtHR takes into consideration the circumstances of the case at hand to determine if the privacy infringing measure of the government is proportionate to the legitimate aim pursued (cf. Ölçer 2008, p. 304). Hirsch Ballin (2012, p. 113) points out that the requirement of 'necessary in a democratic society' also implies an assessment of (1) the proportionality principle and (2) the subsidiarity principle. Law enforcement officials must thus continuously assess

18 See, e.g., ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 66-68, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 55, ECtHR 11 October 2007, *Glas Nadezhda EOOD* and *Anatoliy Elenkov v. Bulgaria*, appl. no. 14134/02, § 46, ECtHR 12 June 2008, *Vlasov v. Russia*, appl. no. 78146/01, § 125.

19 For instance, the ECtHR emphasised in the case of *Malone v. The United Kingdom* that: *"the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention"*. See ECtHR 2 August 1984, *Malone v. The United Kingdom*, app. no. 8691/79, §68.

20 See, e.g., ECtHR 26 April 1979, *Sunday Times v. The United Kingdom*, appl. no. 6538/74, § 67. ECtHR 25 March 1983, *Silver and others v. The United Kingdom*, appl. nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, and 7136/75, §97 and ECHR 26 March 1987, *Leander v. Sweden*, appl. no. 9248/81, §81.

whether the benefit of the application of an investigative method is reasonably balanced with the interference with fundamental rights that may take place (which reflects the proportionality principle) and whether there are no other – less infringing – investigative methods available to gather evidence (which reflects the subsidiarity principle) (cf. Hirsch Ballin 2012, p. 57). As already emphasised in the introduction to this section, this study focuses on whether the regulations of investigative methods are 'in accordance with the law' *in abstracto*. This study does not explore the balancing act described above for the identified digital investigative methods.[21]

The ECtHR typically grants contracting States to the ECHR a 'margin of appreciation' when evaluating whether a privacy infringing measure is necessary in a democratic society.[22] The term 'margin of appreciation' refers to the discretion that the ECtHR is willing to grant national authorities in fulfilling their obligations under the ECHR (see Greer 2000, p. 5). However, the more serious the privacy interferences caused by an investigative method, the more procedural safeguards the ECtHR will prescribe to contracting States to counterbalance the risk of abuse of power by governmental authorities. In such a case, contracting States to the ECtHR have a smaller margin of appreciation in regulating investigative methods that interfere with art. 8 ECHR.

3.2.4 The scale of gravity for privacy interferences

From the case law of the ECtHR, a 'scale of gravity' can be identified regarding the privacy interferences that are caused by the use of investigative methods (see Ölçer 2008, p. 293). Depending on the gravity of the privacy interference that takes place, the ECtHR requires more or less detailed law and procedural safeguards for regulating the investigative methods.[23] The working of this 'scale of gravity for privacy interferences' is illustrated in the Figure 3.1.

21 See also the introduction to section 3.2.

22 See, e.g., ECtHR 25 March 1983, *Silver and others v. The United Kingdom*, appl. nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, and 7136/75, §97 and ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §102.

23 See, e.g., ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, §46, ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §96, and ECtHR 26 October 2000, *Hasan and Chaush v. Bulgaria [GC]*, appl. no. 30985/96, §84.

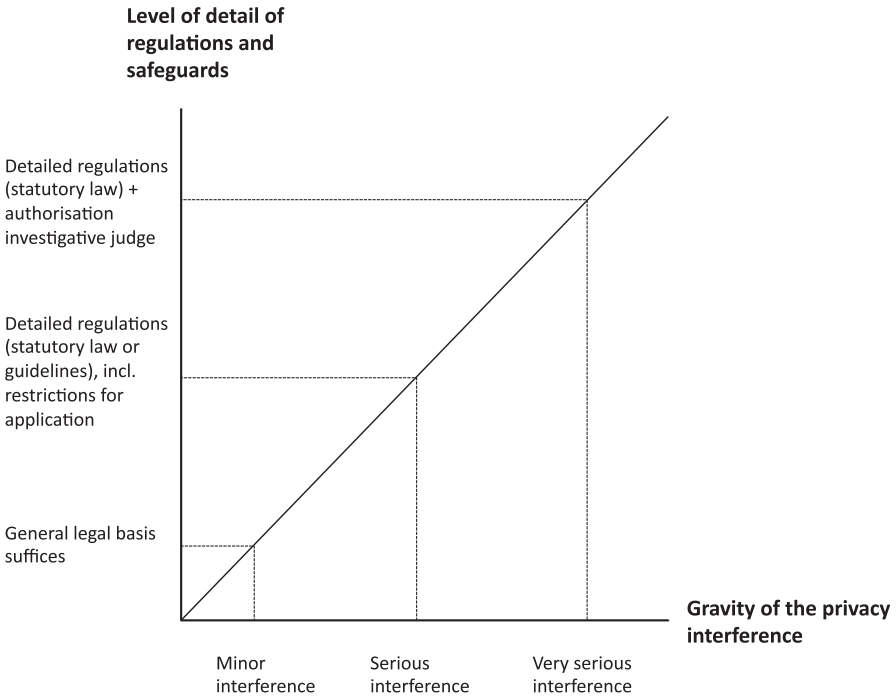

Figure 3.1: Workings of the scale of gravity for privacy interferences.

Figure 3.1 shows how investigative methods that interfere more heavily in the right to privacy generally require a more detailed legal basis in law with more procedural safeguards to protect the right to privacy of the individuals involved (cf. Krabbe, p. 166 in: Harteveld et al. 2004, Ölçer 2008, p. 290, and Gerards 2011, p. 129-130).[24] By requiring regulations that are more detailed with procedural safeguards for investigative methods that interfere with the right to privacy in a serious manner, the ECtHR aims to reduce the risk of abuse of governmental power.[25] The level of detail of the law and procedural safeguards, i.e., the quality of the law that is required for regulating the investigative methods thus depends on the gravity of the privacy interference that occurs when an investigative method is applied. From case law, the following level of detail and procedural safeguards for regulations are distinguished: (1) a general legal basis, (2) detailed regulations in statutory law or guidelines with restrictions for the investigative methods, or

24 The scale of gravity for privacy interferences is in this case presented on a 45 degree angle. However, the scale solely serves to illustrate a legal mechanism. It is not contented the privacy interference can be exactly measured and there is a linear relationship between the gravity of the privacy interference and the required quality of the law.

25 See, e.g., ECtHR 1 July 2008, *Liberty and Others v. The United Kingdom*, appl. no. 58243/00, § 62, ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 61, and ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, § 68

(3) detailed regulations in statutory law with the procedural safeguard of authorisation of an investigative judge.

To illustrate how this scale of gravity is used in case law, two examples of investigative methods that interfere with the right to privacy are presented below: one that interferes in a minor manner and one that interferes more seriously.

Minor interference

The *visual surveillance of an individual in a public place* is an investigative method that interferes with an individual's right to privacy in only a minor manner or, in certain circumstances, not at all.[26] An interference with the right to privacy does take place when personal information that is obtained through public surveillance measures is also *stored in police systems*. Every step in the further processing of personal information once it is stored in police systems amounts to a more serious interference with the right to privacy (see Ölçer 2008, p. 284 and p. 292).[27] However, the investigative method of *the surveillance* of the behaviours of individuals *in public places* itself, does not – or only in a minor manner – interfere with the right to privacy in art. 8 ECHR. With regard to quality of the law, the ECtHR does not state that detailed regulations with procedural safeguards must be implemented in the domestic legal frameworks of member states to protect individuals from this type of governmental interference, even when the recorded information is stored in a police system. A general legal basis that authorises law enforcement officials to use visual surveillance as an investigative method may therefore be sufficient.[28]

Serious interference

The *interception of communications* is an investigative method that seriously interferes with the right to privacy of individuals. This investigative method can be placed at the far right of the scale of gravity for privacy interferences.[29] In relation to the interception of communications, the ECtHR has noted repeatedly that:

26 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 58 with reference to ECtHR 31 January 1995, *Friedl v. Austria*, § 51-52.

27 See also ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 45: *"Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that normally foreseeable."*

28 See, e.g., ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 66.

29 See, e.g., ECtHR 24 April 1990, *Kruslin v. France*, appl. no. 11801/85 and *Huvig v. France*, app. no 11105/84, ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06.

"In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated."[30]

Vis-à-vis the interception of communications, the ECtHR requires – as part of the required 'quality of the law' – that (1) the law is particularly precise and (2) procedural safeguards are implemented within legislation to protect the right to privacy of the individuals involved.[31] More particularly to the latter requirement, the ECtHR considers it important that the investigative method or surveillance measure is authorised by an independent authority, preferably a judge.[32]

It is important to understand the workings of the scale of gravity for privacy interferences and its relation with the regulation of digital investigative methods. Distinct digital investigative methods interfere with the right to privacy as articulated in art. 8 ECHR in their own manner. The ECtHR will thus place the privacy interference that takes place somewhere on the scale of gravity in order to determine the appropriate level of detail and procedural safeguards for each distinct investigative method. The requirements for regulating the identified digital investigative method are further examined in chapter 4.

3.3 Dynamic interpretation of the ECHR

Even though the ECHR was established and concluded within the framework of the Council of Europe in 1950, the treaty is by no means outdated. The reason is that the ECtHR uses '*dynamic, evolutive interpretation*', allowing it to take present-day standards and conditions into consideration. The ECtHR has repeatedly emphasised in its case law that the ECHR is *"a living instrument which should be interpreted according to present-day conditions"* (cf. Lawson & Schermers 1999, p. 50).[33] In subsection 3.3.1, two examples of the dynamic interpretation of convention rights are provided. Section 3.3.2

30 See, e.g., ECtHR 1 July 2008, *Liberty and Others v. The United Kingdom*, appl. no. 58243/00, § 62, ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 61, and ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, § 68.

31 See, e.g., ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 67, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 46 and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 229.

32 See most notably ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 257-267 with reference to ECtHR 26 April 2007, *Dumitru Popescu v. Romania* (no. 2), appl. no. 71525/01, § 71.

33 Emphasis added by the author. The first case in which the ECtHR mentioned that the ECHR should be seen as a living instrument was in ECtHR, 25 April 1978, *Tyrer v. The United Kingdom*, appl. no. 5856/72 § 31. As Letsas (2013, p. 108) points out, the ECtHR 'very rarely' inquires what was thought be acceptable conduct when the ECHR was drafted or what specific rights the drafters of the ECHR intended to protect.

discusses the relevance of the interpretation method for the regulation of digital investigative methods.

3.3.1 Two examples of the dynamic interpretation of convention rights

The dynamic, evolutive interpretation of the convention rights articulated in the ECHR is clearly visible in case law. Two examples are provided to illustrate the evolutive interpretation with regard to convention rights and the Internet.[34]

First, the ECtHR has repeatedly stated in its case law that the Internet plays an important role in enhancing public access to and the dissemination of information, which are both part of the right to freedom of expression that is articulated in art. 10 ECHR.[35] This idea is clearly visible in the 2015 case of *Cengiz and Others v. Turkey*.[36] In this case, the ECtHR found that a blanket order to block YouTube affected the applicants' right to receive and impart information and ideas. This blanket blocking order thus violated the right to freedom of expression in art. 10 ECHR.[37]

Second, the dynamic, evolutive interpretation of convention rights is clearly visible in case law with regard to the right to privacy and the interception of communications by use of the Internet. At first, the ECtHR dealt with cases concerning the right to respect for private life and the right to respect for correspondence in relation to the interception of communications made by telephone. In 2007, the evolutive interpretation became clear when the ECtHR stated in the case of *Copland v. The United Kingdom* that *e-mails* and *information derived from the monitoring of personal Internet usage* are also protected under the right to respect for correspondence in art. 8 ECHR.[38] This second example illustrates that the dynamic, evolutive interpretation of convention rights can be particularly important for digital investigative methods, which often interfere in the right to privacy in new manners.

---

34 See also the report 'internet case-law of the European Court of Human Rights' of the Council of Europe (June 2015) for a more general and extensive overview of case law. Available at: http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf (last visited on 24 June 2016). See also the recently published factsheet of the ECtHR on 'new technologies' with a list of case law from June 2016. Available at: http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf (last visited on 24 June 2016).

35 See, e.g., ECtHR 10 March 2009, *Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom*, appl. nos. 3002/03 and 23676/03, § 27, ECtHR 18 December 2012, *Ahmet Yildirim v. Turkey*, appl. no. 3111/10, § 48-49.

36 See ECtHR 1 December 2015, *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11.

37 See ECtHR 1 December 2015, *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11. See also ECtHR 18 December 2012, *Ahmet Yildirim v. Turkey*, appl. no. 3111/10.

38 ECtHR 3 April 2007, *Copland v. The United Kingdom*, appl. no. 62617/00, § 41.

3.3.2 Relevance for digital investigative methods

The dynamic, evolutive interpretation of convention rights is an important concept for the regulation of digital investigative methods based on art. 8 ECHR. From this concept, it follows that the ECtHR does not only interpret convention rights based on the text of the ECHR itself or its historical meaning. Following the preamble of the convention, the "maintenance and further realisation of Human Rights and Fundamental Freedoms" is the aim to be pursued by the convention. The ECtHR interprets convention rights in order to realise this goal.

This 'teleological interpretation' of convention rights features in "virtually all judgements of the ECtHR", according to Senden (2011, p. 58). This means that the textual interpretation of convention rights can at times be 'overruled' by the ECtHR to ensure the protection of fundamental individual rights (see Senden 2011, p. 53). The ECtHR also uses the 'consensus method' and the 'principle of autonomous interpretation' to interpret convention rights according to their present-day standards. These methods of interpretation are further considered below.

The 'consensus method' means that the ECtHR compares the laws of contracting States to determine whether consensus on a certain issue can be found. If this consensus is found, the ECtHR can adopt an interpretation that is in line with this consensus (see Senden 2011, p. 67). For instance, if many contracting States require a warrant to conduct a computer search, the ECtHR may refer to that legislation and specify that a warrant is part of the required quality of the law according to present-day standards.

It can also occur that contracting States to the ECtHR take a restrictive interpretation of the scope of protection under art. 8 ECHR and provide their governmental investigative authorities with broad investigative powers, which the ECtHR may not deem to be desirable. In such a case, the ECtHR need not grant discretion, follow consensus, or assign decisive importance to what a respondent State considers an acceptable interpretation of standards in the circumstances at hand. The ECtHR then interprets the law *autonomously* (cf. Letsas 2013 in: Føllesdal, Peters & Ulfstei 2013, p. 108). Senden (2011, p. 78) explains that if the ECtHR were to take a different approach, it would be dependent on national classifications for the regulation of investigative methods, which would in turn undermine the ability of the ECHR to provide a minimum level of protection for human rights. In the context of the regulation of digital investigative methods, the autonomous interpretation of convention rights may allow the ECtHR to decide that it is desirable to expand the protection of the right to privacy to cover certain aspects of the right to privacy when digital investigative methods are applied. In addition, the ECtHR can also decide that certain regulations and procedural safeguards are required to adequately regulate digital investigative methods.

In brief, a dynamic reading of the ECHR provides the degree of flexibility necessary for the ECtHR to interpret convention rights in a rapidly changing environment (see Dzehtsiariou 2011, p. 1732). It also enables the ECtHR to both appraise interferences with convention rights when digital investigative methods are applied according to present-day standards and conditions and formulate any desirable regulations that it deems necessary.[39] The same is true of teleological and autonomous interpretation applied by the ECtHR. All contracting States to the ECHR must then meet the required quality of the law by implementing the normative requirements in their domestic legal frameworks.

3.4 Chapter conclusion

The aim of this chapter was to identify the basic framework containing the normative requirements for the regulation of investigative methods from art. 8 ECHR (RQ 2). To answer the research question of this chapter, (1) the scope of art. 8 ECHR, (2) the conditions as stipulated in art. 8(2) ECHR, and (3) the interpretative approaches of the ECtHR to convention rights were examined.

The analysis showed that investigative methods that interfere with the right to privacy must meet three conditions: (1) they must have a legitimate aim, (2) they must be in accordance with the law, and (3) they must be necessary in a democratic society. In relation to regulating investigative methods, the second condition of being '*in accordance with the law*' is most important. This second condition requires that the regulations for the investigative methods (1) are *accessible*, (2) are *foreseeable*, and (3) meet a certain *quality of the law*. Further in this study, these normative requirements are deployed as the framework against which the regulation of investigative methods should be tested.

In relation to the required quality of the law, it is important to note that the gravity of a privacy interference and the accompanying quality of the law are interpreted in conformity with present-day standards and conditions. When the gravity of a privacy interference that results from applying an investigative method changes due to technological developments, the required quality of the law should change accordingly. The gravity of privacy interferences and the accompanying desirable quality of the law for the identified digital investigative methods are further examined in chapter 4.

39 At the same time, in the context of the regulation of investigative methods, contracting States to the ECtHR may regard an autonomous interpretation of convention rights as a risk to their sovereign right to regulate governmental powers that are used for evidence gathering purposes in criminal investigations.

4 The right to privacy and digital investigative methods

This chapter aims to answer the third research question (RQ 3): *Which quality of law is desirable for the identified digital investigative methods?* The chapter is concerned with correctly identifying the interference with the right to privacy that takes place when the identified digital investigative methods are applied. Based on that interference, the desirable quality of law is formulated. Three steps are taken to answer RQ 3.

In the first step, ECtHR case law regarding investigative methods that are most similar to the identified digital investigative methods is analysed. As no specific case law is available with regard to the identified digital investigative methods, the case law of similar investigative methods is analysed to determine which type of regulations are required. The point of departure is that the basic structures of both digital investigative methods and their non-digital counterparts are comparable and that requirements for digital methods can be extrapolated from existing case law concerning non-digital methods. In accordance with that point of departure, the existing regulations for non-digital methods in Dutch law, which will be examined in the following chapters, can potentially provide a basis for regulating digital investigative methods. The aim is to determine whether Dutch law requires any amendments or additions to existing regulations, because of differences between digital and non-digital variants, which may bring with them that the existing bases are not adequate as they stand for digital variants.

In the second step, the gravity of the privacy interferences involved in the application of the distinct digital investigative methods is analysed. It is then determined whether the quality of the law that is required for counterpart non-digital investigative methods also 'fits' the digital investigative methods. Bearing in mind the restriction set forth in section 1.3, it should be recalled that this study does not examine desirable regulations for datamining techniques. However, the further processing of personal data once it is stored in police systems is taken into consideration, because they can influence both the gravity of the privacy interference and the appropriate quality of the law for the identified digital investigative methods. The scale of gravity for privacy interferences as presented in subsection 3.2.4 will be used to position the digital investigative methods accordingly. As explained in chapter 3, the ECtHR prescribes the detail of law and procedural safeguards for regulating the investigative methods, depending on the gravity of the privacy interference that takes place. The identified digital investigative methods interfere with the right to privacy in their own manner and should be placed at a specific point on the scale of gravity for privacy interferences to determine which quality of the law is appropriate.

In the third step, detected misalignments in the appreciation of the gravity of the privacy interference and quality of the law requirements derived from case law concerning counterpart investigative methods and that of privacy interferences caused by digital investigative methods are analysed to determine whether a different level of detail in regulations and different safeguards are desirable for the identified digital investigative methods. In the conclusion of the chapter, a table is provided that indicates which level of detail for regulations and procedural safeguards are desirable for the identified digital investigative methods. The results of this analysis provide the basis for determining (in chapters 5 to 8) whether the Dutch approach to regulating digital investigative methods is correct and meets the identified desired quality of the law for the investigative methods.

The structure of this chapter is based on the four investigative methods, each of which is examined in its own section. The structure is thus as follows: section 4.1 examines the gathering of publicly available online information; section 4.2 analyses the data production orders that are issued to online service providers; section 4.3 explores online undercover investigative methods; and section 4.4 examines hacking as an investigative method. Finally, section 4.5 presents a summary of the findings of the chapter.

4.1 Gathering publicly available online information

This section analyses the gravity of the privacy interferences that take place when law enforcement officials gather publicly available online information. Previously, the gathering publically available information in the course of criminal investigations was not a real issue, since the information-gathering capabilities of law enforcement authorities were limited to certain sources. However, the proliferation of publically available information online and the development of modern technologies that enable law enforcement authorities to gather and process large quantities of data have given rise to more intrusive privacy interferences (see WRR 2016).

ECtHR case law regarding counterpart investigative methods in this regard is examined in subsection 4.1.1. In subsection 4.1.2, the digital equivalents of these investigative methods are further analysed in their relation to the right to privacy. Subsection 4.1.3 then concludes the section by determining which quality of the law is *desirable* for the gathering of publicly available online information.

4.1.1 The right to privacy regarding similar investigative methods

The following subset of the digital investigative method was distinguished in chapter 2: (A) the manual gathering of publicly available online information, (B) the automated gathering of publicly available online information, and (C) observing the online behaviours of individuals. This subsection

examines case law with regard to similar investigative methods as compared to the gathering of publicly available online information.

The following investigative methods are considered similar to their digital counterparts: (A) the gathering of information from open sources, (B) the pre-emptive storage of personal information for law enforcement purposes, and (C) the visual surveillance of the behaviours of individuals in the physical world.

A The gathering of information from open sources

Open source information can be defined as information that anyone can lawfully obtain by request, purchase, or observation (cf. Eijkman & Weggemans 2012, p. 287).[1] An important case that reflects the privacy interference that takes place when open source information is gathered by law enforcement officials is the 2006 case of *Segerstedt-Wiberg and Others v. Sweden* (henceforth *Segerstedt-Wiberg*).[2] In this case, the Swedish Security Police collected information about individuals by (a) observing these individuals' public activities, (b) amassing newspaper articles about them, and (c) gathering public decisions taken about them by public authorities. The individuals involved complained to the ECtHR that storing this information in the Security Police files constituted an unjustified interference with their right to respect for private life.[3] The Swedish government contended that the information was publicly available and therefore questioned whether the information that was stored interfered with the right to respect for private life as protected under art. 8(1) ECHR.[4]

In the case of *Segerstedt-Wiberg*, the ECtHR decided that the storage of public information in the Security Police register and release of that information constituted an interference in the private lives of the individuals involved. The ECtHR emphasised that the fact that the data was public did not negate the interference, "*since the information had been systematically collected and stored in files held by the authorities.*"[5] The ECtHR also decided in other cases that "*public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities*".[6]

1 Eijkman & Weggemans refer to the National Open Source Enterprise, Intelligence Community Directive 301 of July 2006 for this definition.

2 ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00.

3 ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00, § 70.

4 ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00, § 71.

5 ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00, § 72.

6 See ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00, § 72 with reference to ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 43. See also the case law with regard to the storage of information in police systems that does not concern public information: ECHR 26 March 1987, *Leander v. Sweden*, appl. no. 9248/81, § 48, ECtHR 4 May 2000, ECtHR 13 November 2012, *M.M. v. The United Kingdom*, appl. no. 24029/07, § 87 and ECtHR 17 December 2009, *Gardel v. France*, appl. no. 16428/05, § 58.

The ECtHR thus particularly test whether the information is (1) *systematically gathered* and (2) *stored in a police system* to determine whether an interference took place with the right to respect to private life. This test is also visible in other case law. For instance, the ECtHR found that no interference with the right to respect for private life takes place when law enforcement officials take pictures of an individual during a public demonstration, without storing that information in a police system (cf. De Hert 2005, p. 75).[7] The ECtHR clearly takes an individual's 'reasonable expectation of privacy' into consideration in its case law concerning the surveillance of individuals in their public lives.[8] The court has repeatedly stated in case law that *"a person who walks down the street will, inevitably, be visible to any member of the public who is also present"*.[9] The member of the public who is observing others can apparently also be a law enforcement officer. The fact that law enforcement officers use technological means, such as CCTV cameras, to monitor activities in a public scene does not make a difference, according to the ECtHR.[10]

When the information obtained from a public scene is *stored* in a police system, an interference with the involved individual's right to respect for private life takes place.[11] Case law of the ECtHR regarding the processing of stored recordings from CCTV images indicates that every step in the further processing of personal information once it is stored in police systems amounts to a more serious interference with the right to privacy (see Ölçer 2008, p. 284 and p. 292).[12] For example, in the case of *Peck v. The United Kingdom*, an individual who was 'in a state of distress' and wielding a knife was filmed by a CCTV camera.[13] These behaviours were filmed by a CCTV camera. Law enforcement officials then released to footage to a television

7 Citing ECommHR, *Pierre Herbecq and the Association Ligue des droits de L'homme v. Belgium*, Decision of 14 January 1998 on the applicability of the applications no. 32200/96 and 32201/96 (joined), Decisions and Reports, 1999, p. 93-98 in which the Commission finds that no privacy interference takes place when photographic equipment is used that does not record the visual data. See also ECtHR 31 January 1995, *Friedl v. Austria*, § 51-52.

8 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57. See also ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38.

9 Idem.

10 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57. See also ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38.

11 See, e.g., ECtHR 18 February 2000, *Amann v. Switzerland*, appl. no. 27798/95, § 65, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 43, ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 59-60, ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 62-63, ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38 and 40-41, and ECtHR 17 December 2009, *Gardel v. France*, appl. no. 16428/05, § 62.

12 See also ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 45: *"Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that normally foreseeable."*

13 See ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 62.

show without informing and anonymising the individual involved.[14] It turned out the individual was contemplating to commit suicide. The ECtHR found that, in this case, the processing of personal information took place in a manner that could not be foreseen by the individual involved, which gave rise to a serious interference in his right to privacy.[15]

Required quality of the law

When deciding whether the storage of personal data obtained from public places amounts to an interference with the right to privacy, the ECtHR often refers to the Council of Europe's convention for the protection of individuals with regard to the automatic processing of personal data to discuss the required quality of the law.[16] Data protection regulations restrict the systematic collection and storage of personal information in police systems and can be considered as a framework representing the ECtHR's required quality of the law.

For instance, in the case of *Rotaru v. Romania*, the ECtHR specifically considered which restrictions were available in the domestic legislation of Romania with regard to the systematic collection and storage of personal data by law enforcement officials.[17] The court reviewed (1) which provisions were available concerning the individuals who were authorised to consult the stored files containing personal data and (2) whether provisions were available concerning the retention period of these files.[18] These restrictions were based on data protection regulations and can be considered as the required quality of the law for the gathering of personal data from open sources.

Storage of personal data v. processing of personal data

The difficulty with the case law of the ECtHR regarding the systematic gathering of information from open sources is that the ECtHR does not make a clear distinction between (a) the *storage of personal information* in police systems and (b) the *processing of personal information* by law enforcement officials (cf. De Hert 2005, p. 75). Since the storage of data in a police system is an interference, the question arises whether merely processing personal information taken from public sources (without storing it in a police file)

14 ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 62.

15 See ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 62-63.

16 Treaty of 28 January 1981, CETS no.108. See, e.g., ECtHR 18 February 2000, *Amann v. Switzerland*, appl. no. 27798/95, § 65, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 43, ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57 and ECtHR 17 December 2009, *Gardel v. France*, appl. no. 16428/05, § 27.

17 ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 43: "*Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities*".

18 ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 57.

amounts to an interference with the right to private life. An example of this situation is when a law enforcement official takes a picture of an individual in a public place without storing the information in a police system. As explained above, it is likely the court will reason this surveillance measure is both not applied systematically and information is not stored in a police system. In that situation, no interference takes place with art. 8(1) ECHR.

However, data protection regulations within the European Union already apply when personal information is *merely processed* by law enforcement officials.[19] The application of these regulations do not require (1) the systematic collection and (2) the storage of personal information in a police system. For example, when law enforcement officials manually gather online information about a suspect by use of Google based on the suspect's name, data protection regulations apply. For instance, the investigative activity can only take place with a legitimate aim (such as gathering evidence in a criminal investigation). This means that data protection regulations apply earlier for many law enforcement authorities, i.e., all law enforcement authorities in the EU, than the ECtHR acknowledges. De Hert (2005) presents a more detailed discussion on this topic. It is important to realise that EU data protection regulations provide more protection to the individuals involved, because the threshold to apply these EU data protection regulations are lower than the one required by the ECtHR. This is illustrated in Figure 4.1, which is an adaptation of the scale of gravity for privacy interference and the required quality of the law in Figure 3.1.

19 See the Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 P. 0031 – 0050 and its proposed successor the Proposal for a regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), 25 January 2012, COM(2012) 11 final 2012/001 (COD). See also with regard to data protection regulations for law enforcement authorities within the European Union: the proposal on the on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 010 final 2012/0010 (COD).

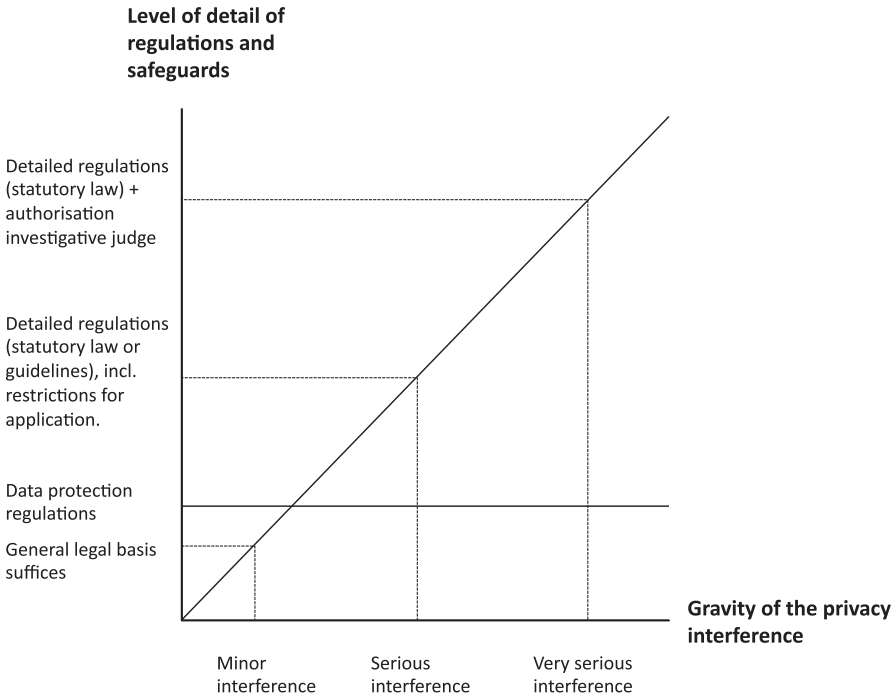

Figure 4.1: Scale of gravity for privacy interferences with accompanying quality of the law and data protection regulations.

Figure 4.1 illustrates how data protection regulations present a baseline for the quality of the law for the regulation of investigative methods that involve the processing of personal data. Data protection regulations can thereby restrict the application of investigative methods, even when even when the investigative method itself does not interfere with the right to privacy in a serious manner by art. 8 ECHR standards.

B The pre-emptive storage of personal information

In 2008, the ECtHR dealt with the legitimacy of the pre-emptive storage of personal information for law enforcement purposes in its case law.[20] The case of *S. and Marper v. The United Kingdom* is further below examined in order to determine the gravity of the privacy interference that takes place when information is pre-emptively stored in police systems. The quality of the law that the ECtHR finds appropriate for such an investigative method is also examined. The investigative method can be distinguished from open source information gathering under A, by the fact that this investigative

20 See ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04.

method regards to use of a database by law enforcement officials based on personal information that has been previously obtained and stored for later use for law enforcement purposes.

In the case of *S. and Marper v. The United Kingdom*, the pre-emptive storage of personal information in a police system concerned fingerprints and DNA materials that were taken from individuals following their arrest in the United Kingdom. These items were stored in a police system, which meant they could be used later in time for law enforcement purposes. When the applicants requested that the materials be deleted from the database, the government in the United Kingdom refused to do so. The case was eventually brought to the ECtHR.

To decide whether the storage of the data interfered with the applicants' right to privacy, the ECtHR took the following four factors into consideration: (1) the specific context in which the information at issue had been recorded and retained, (2) the nature of the records, (3) the way in which these records were used and processed, and (4) the results that could be obtained with the storage of the information.[21]

In its decision, the ECtHR determined that DNA materials should be seen as sensitive information, because they include details concerning an individual's health. In addition, DNA profiles derived from those materials provide a means for identifying genetic relationships between individuals as sensitive information. For these two reasons, the storage of the DNA materials was found to be an interference with the right to respect for private life as articulated as an object of protection in art. 8 ECHR.[22] With regard to the storage of fingerprints, the ECtHR concluded that the information is less sensitive than DNA materials. However, the fingerprints that were taken in criminal proceedings were permanently stored in a police database and regularly processed by automated means for criminal identification purposes, which amounted to an interference with art. 8(1) ECHR.[23]

Required quality of the law

With regard to the quality of the law, the ECtHR requires specific safeguards in the domestic legal frameworks of contracting States in order to avoid governmental abuse of the pre-emptive storage of sensitive materials. In *S. and Marper v. The United Kingdom*, the ECtHR required that (1) no more data is gathered than necessary for the investigation of specific crimes, (2) a specific

21 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 67.

22 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 72-75. The ECtHR also considered the storage of fingerprints – in connection with an identified or identifiable individual – in a police system as an interference with regard to the right to respect for private life. See ECtHR 18 April 2013, *M.K. v. France*, appl. no. 19522/09, § 32.

23 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 86.

retention period for the storage of personal data is in place (which is differentiated based on the seriousness of the offence), and (3) the involved individuals have the possibility to access and request deletion of the stored records.[24] It is noteworthy that these requirements are similar to those that generally apply to data protection regulations.[25]

An important consideration in the case of *S. and Marper v. The United Kingdom* is that the ECtHR emphasised that the *indiscriminate* pre-emptive storage of personal information also encompasses the collection of personal information from individuals who are not suspected of crime. This is deemed problematic by the ECtHR, because individuals who are not suspects must be presumed innocent and should not be subjected to governmental interferences in their private lives.[26] For that reason, the ECtHR carefully scrutinises the pre-emptive collection of sensitive information for law enforcement purposes in light art. 8 ECHR to decide whether the storage of information is proportionate considering the law enforcement aim (the prevention of disorder can crime) that is pursued.[27]

C Visual surveillance of the behaviours of individuals in the physical world

The case of *Segerstedt-Wiberg* is also relevant for the visual surveillance of individuals by law enforcement officials in the physical world; given that the information that can be obtained by observation in a public context is also considered as "open source information" (cf. Eijkman & Weggemans 2012, p. 287).[28] Other case law of the ECtHR concerning the surveillance of individuals in public places is also relevant.[29] Essentially, the ECtHR has made it clear in these cases that individuals who knowingly expose themselves to any other member of the public who can take notice of their behaviours in public are not necessarily protected by the right to respect for private life as meant in art. 8(1) ECHR.

24 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 103.

25 See, e.g., the Directive 95/46/EC of 24 October 1995 and the Proposal for a regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), 25 January 2012, COM(2012) 11 final 2012/001 (COD).

26 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, App. nos. 30562/04 and 30566/04, § 122. See also ECtHR 18 April 2013, *M.K. v. France*, appl. no. 19522/09, § 39.

27 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 99. See also ECtHR 18 April 2013, *M.K. v. France*, appl. no. 19522/09, § 28.

28 Eijkman & Weggemans refer to the National Open Source Enterprise, Intelligence Community Directive 301 of July 2006 for this definition.

29 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57. See also ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38.

However, the ECtHR has also clarified in these cases that the right to private life in art. 8(1) ECHR provides for *"a zone of interaction of a person with others, even in a public context"*.[30] The background of this aspect of the right to privacy is that individuals must be able to engage in relationships with others – even in public – without arbitrary governmental interferences.[31] This statement seems to contradict the previous statement that no interference with the right to privacy takes place when information is obtained from a public place by the use of visual surveillance measures.

Nonetheless, here again the ECtHR considers it important that the information that is obtained from visual surveillance is also *stored in police systems* in order to speak of an interference with the right to respect for private life taking place.[32] The further processing of that information amounts to a more serious privacy infringement.[33]

Required quality of the law

With regard to the observation of an individual's movements in public, ECtHR case law has not required that specific procedural safeguards must be implemented in the domestic legal frameworks of contracting States. A general legal basis for using the investigative method may therefore suffice.

For instance, in the context of the use of GPS surveillance to monitor the movements of an individual and his accomplice in a car, the ECtHR found in the case of *Uzun v. Germany* that a general legal basis and authorisation by law enforcement officials to apply the investigative method were sufficient. Although the duration of the surveillance measure was not concretely restricted by statutory law, the proportionality principle that was applied by law enforcement officials ensured that this duration was sufficiently restricted.[34] However, when deciding on the legitimacy of the investigative method, the ECtHR did specifically take into consideration (1) the nature, scope, and duration of the surveillance measures; (2) the grounds required for ordering them; (3) the authorities competent to permit, carry out, and supervise the measures; and (4) the kind of remedy provided by the national

30 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 56. See also e.g., ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 36, ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 43, and ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, § 64.

31 See, e.g., ECtHR 12 January 2010, *Gillian and Quinton v. The United Kingdom*, appl. no. 4158/05, § 61 and ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 44.

32 See, e.g., ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57. See also ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38.

33 See, e.g., ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 51-53.

34 See ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 69-70. The court explicitly noted that surveillance with a GPS device is distinguished from other methods of surveillance that disclose more information person's conduct, opinions or feelings (see ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 52).

law.[35] The ECtHR tested whether German law enforcement authorities took these factors into consideration in *concreto*, based on the circumstances at hand. It did not require detailed regulations in statutory law or guidelines for the investigative method. Instead, a general legal basis may suffice, as long law enforcement officials consider these factors when applying the investigative method. To a large extent, the manner in which these public surveillance measures are regulated in law is thus left to the discretion of contracting States to the ECtHR.

4.1.2 The right to privacy and gathering publicly available online information

The digital investigative method is distinguished in: (A) the manual gathering of publicly available online information, (B) the automated gathering of publicly available online information, and (C) observing the online behaviours of individuals.

These three digital investigative methods are further examined to identify the gravity of the privacy interference that takes place when they are applied. It is also examined whether, based on the gravity of the privacy interference, these digital investigative methods fit the framework developed in ECtHR case law for their counterpart methods examined above.

A Manual gathering of publicly available online information

On the one hand, the investigative method of the manual gathering of publicly available online information is similar to the gathering of information from open sources that discussed in subsection 4.1.1. The similarity is that both investigative methods concern evidence-gathering activities with regard to personal information that is publically available. In its most elementary form, the manual gathering of publicly available online information takes place when a law enforcement official looks for information about an individual on the Internet by typing key words into an internet search engine, such as Google.com.[36]

On the other hand, the manual gathering of publicly available online information that takes place today is very different from the gathering of data from open sources that takes place offline. The interference with the right to privacy when the method is applied online to open sources takes place in a different context. The following three reasons are identified in relation to why the collection of publicly available information online interferes with the right to privacy in a different manner its non-digital counterpart.

35 See, e.g., ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 63 and ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, §68.

36 See subsection 2.2.2 under A1 for a more extensive description of the investigative method.

(1) The Internet allows law enforcement officials to collect information on a much *greater scale* than before (cf. WRR 2016, p. 40). The large amounts of information about an individual that may nowadays be available online, should be taken into consideration when determining the gravity of the privacy interference (cf. Koops 2013, p. 663). The information can also be particularly sensitive, because pictures, opinions, feelings, and political views of individuals can be gathered from publicly accessible online sources (such as web forums and social media websites).
(2) Computers and the Internet make it possible to collect information *globally* and then to *conveniently* store relevant parts of it in a police system for evidence purposes. The information gathering can take place across State borders and is not as labour-intensive as before. Furthermore, the costs associated with storing and processing information continue to decrease (cf. WRR 2016, p. 41).
(3) Computers and the Internet make it possible for law enforcement officials to *process the collected information* in order to gain better insights into the private lives of individuals. Computers can help law enforcement officials to 'interpret' collected data by making an automatic selection and visualising the gathered data (cf. Koops 2013, p. 662). For example, law enforcement officials can gain insight into an online network of individuals by examining their friendship connections on social media websites.

Gravity of the privacy interference
It has been pointed out above that the ECtHR interprets the right to privacy *dynamically* and *evolutively* according to *present-day standards*. When technological developments are taken on board, it should be concluded that the gravity of privacy interference has increased when publicly available information is gathered manually.

At the same time, a mitigating factor for the gravity of the privacy interference that the ECtHR may take into consideration is that – to a large extent – the information is often 'knowingly exposed' by the individuals involved. The ECtHR may therefore take a person's reasonable expectation of privacy into consideration when deciding on the gravity of the privacy interference that may take place when law enforcement officials collect such information.

Alignment with the existing required quality of the law
The analysis of case law related to offline gathering of publicly available information subsection 4.1.1 indicates that the ECtHR only speaks of a privacy interference when information is systematically gathered and stored in police systems. It is possible that in an online context, law enforcement officials gather information sooner in a systematic manner than in an offline context. The reason is that more information and more diverse (and possibly sensitive) information is readily available on publicly available sources. However, one can nevertheless argue that *merely processing* publicly available online information that has been manually obtained in a single internet

search in itself does not necessarily interfere with the right to privacy as meant in art. 8(1) ECHR (cf. O'Floinn & Ormerod 2011, p. 777 and Koops 2013, p. 659).

Considering the increased amounts and broader diversity of information that is available online nowadays and the development of data protection regulations in the EU however, the position of the ECtHR (based on investigative methods that were applied in an offline context) should no longer hold. It would appear to instead be more appropriate for the ECtHR to recognize the possibility that online gathering of publicly available information is intrinsically more likely to interfere with privacy in a graver manner and this gravity will fluctuate depending on the type of information at issue. The ECtHR should consider to adopt the more modern data protection regulations, which apply when information is processed by law enforcement officials. These data protection regulations restrict the evidence gathering activity even when no information is stored in a police system and seem to be sensitive to the alternate context of publicly available sources in the digital world.

B Automated gathering of publicly available online information

Automatic data collection systems pre-emptively gather information from relevant online sources every day. This automated gathering of publicly available online information is an investigative method that can aid law enforcement officials by making relevant information available to them. In addition, these automated systems can process the collected information and present the officials with more relevant results (including quick visualizations of the information).[37]

Gravity of the privacy interference

A privacy interference clearly takes place when automated data collection systems are used. The storage of information in itself interferes with the right to privacy as articulated in art. 8 ECHR.[38]

The factors developed in the case of *S. and Marper v. The United Kingdom* for DNA and fingerprints are helpful for determining the gravity of the privacy interference when automated gathering of publicly available online information is at issue. These factors, which are elaborated on in subsection 4.1.1 (under B), include: (1) the specific context in which the information at issue has been recorded and retained, (2) the nature of the records, (3) the way in which these records are used and processed, and (4) the results that may be obtained with the storage of the information.[39] In the case of

37 See subsection 2.2.2 under A2.

38 Providers of commercial data collection systems already download and further process publicly available online information every day in order to provide the best search results for their clients.

39 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §67 and §119.

S. and Marper v. The United Kingdom, the ECtHR found that the indiscriminate collection of information about individuals is a measure that seriously interferes with the right to privacy of the individuals involved.[40] When automated data collection systems are used, an indiscriminate collection of information about individuals also takes place. Developments in technology also make it possible to obtain an intricate picture of certain aspects of the private lives of the individuals involved.

However, the gathering of publicly available online information is not nearly as sensitive as the gathering and processing of DNA materials, as was the case in *S. and Marper v. The United Kingdom*. As DNA material can reveal details concerning an individual's health and genetic relationships with others, they are considered to contain particularly sensitive information.[41] In contrast, publicly available online information need not be as sensitive as this type of information whilst individuals often knowingly expose information on the Internet by themselves. For that reason, the automated gathering of online information is possibly considered not as privacy intrusive as the system that was in place in the case of *S. and Marper v. The United Kingdom*.

Nonetheless, large amounts of information are gathered by automated data collection systems and processed to obtain detailed insights into the lives of the individuals involved. In *S. and Marper v. The United Kingdom*, the ECtHR warned that the potential benefits of the extensive use of "modern technology" for law enforcement purposes should be carefully balanced against private life interests.[42] This warning should be kept in mind when articulating the desirable quality for the law of the investigative method of automated gathering of publicly available online information. In addition, in both investigative methods information is indiscriminately pre-emptively stored in police systems for law enforcement officials, which necessitates a strict test of the quality of the law.

Alignment with the existing required quality of the law

The investigative method that concerns the non-digital collection of personal information in *S. and Marper v. The United Kingdom* and the automated gathering of publicly available online information are both intrusive, but they interfere with the right to privacy in different manners.

However, the data protection principles that were applied in the *S. and Marper v. The United Kingdom* case may essentially also be appropriate for the automated gathering of online information. In addition, given that the preemptive collection of information may involve (a large number of) a third

40 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §120.

41 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 72-75.

42 See ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §112: *"The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard."*

party, about whom information is also gathered, a heightened proportionality test also appears to be appropriate here.[43] The legislative requirements for the pre-emptive collection of personal data as framed in *S. and Marper v. The United Kingdom* may therefore also be suitable for the pre-emptive collection of publicly available online information.

C Observing online behaviours of individuals

Law enforcement officials can also observe the online behaviours of individuals on publicly accessible places on the Internet. For instance, law enforcement officials can observe an individual's public posts to online platforms such as social media services, online forums, and chat services.[44] The observation concerns online behaviours that take place in real-time, not those that occurred in the past. For the gathering of information that took place in the past, the investigative method of the manual gathering of publicly available online information is applied.

Gravity of the privacy interference

The privacy interference that takes place when law enforcement officials observe an individual's online behaviour is comparable to the interference when they use visual surveillance to observe an individual's movements in public life. The ECtHR has made it clear in case law that as part of the right to privacy, individuals must be able to engage in relationships with others – even in public – without the interference of the government.[45] There is no reason to assume that this aspect of the right to privacy would not apply to the behaviours of individuals in online environments.

The factors provided by the ECtHR for determining the gravity of the privacy interference when behaviours are observed also appear suitable for an online context. These factors are as follows: (1) the nature, scope, and duration of the possible measures; (2) the grounds required for ordering the measures; (3) the authorities competent to permit, carry out, and supervise the measures; and (4) the kind of remedy provided by the national law.[46] The ECtHR does not require detailed regulations for the investigative method. A general legal basis may thus suffice, as long the factors are used in practice when law enforcement officials apply the investigative method.

43 As explained in the introduction to section 3.2, the test whether the interference is 'necessary in a democratic society' is still relevant.

44 See subsection 2.2.2 under A3.

45 See, e.g., ECtHR 12 January 2010, *Gillian and Quinton v. The United Kingdom*, appl. no. 4158/05, § 61 and ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 44.

46 See ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 63. These procedural safeguards are repeated in ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, §68.

Alignment with the existing required quality of the law
An important difference between observing the behaviours of individuals online and observing them in the physical world is that in an online context law enforcement officials can quickly learn about public behaviours that occurred *in the past* (cf. Oerlemans & Koops 2012, p. 46). For example, they can observe statements that individuals are currently making on social media or internet forums as well as look up statements that these individuals made in the past. In that way, much more information is available to law enforcement officials compared to when, for instance, they observe the movements of an individual in the physical world.

In addition, observing the online behaviours of an individual appears more straightforward, since the investigative method can be automated and does not require the law enforcement officials to physically move from one place to another. This investigative method is thus different in nature from its counterpart in the physical world.

Nevertheless, it is still not likely that the ECtHR will regard the online observation as an intrusive investigative method that is comparable to when, for instance, the private communications of a person are secretly wiretapped.[47] The ECtHR will take the reasonable expectation of privacy of individuals into consideration when law enforcement officials gather information that is publicly available to anyone. Since the privacy interference that takes place when public behaviours are observed is not considered as particularly serious, the ECtHR is not expected to require more detailed regulations with specific procedural safeguards for the digital investigative method.

4.1.3 Desired quality of the law

This subsection determines the *desirable* quality of the law based on the gravity of the privacy interference that takes place when publicly available online information of individuals is collected in the three modalities discussed above. In general, it should be observed that much more 'open source' information is publically available on the Internet than in an offline context. The ability to collect information from individuals located anywhere in the world is also novel.

However, the privacy interference that takes place when the investigative methods discussed above are applied can generally be placed at the low end of the scale of gravity for privacy interferences. The main reason is that case law indicates that the ECtHR takes into consideration the fact that information is publicly available to anyone, including law enforcement authorities. Based on the examined case law concerning non-digital counterparts, it is not likely that the ECtHR will require detailed regulations with certain procedural safeguards for the gathering of publicly available online

47 See, e.g., ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, §66.

information, so that more general bases may suffice. It was argued that, taking into consideration present-day standards, data protection regulations should be applicable to the processing of personal information.[48]

The desirable quality of the law depends on how the publicly available online information is gathered. The quality of the law that is in my view desirable for regulating the information-gathering methods is presented below.

A Manual gathering of publicly available online information

With regard to the manual gathering of publicly available online information, a general legal basis for applying the investigative method coupled with data protection regulations may suffice. As only a minor privacy interference takes place when this investigative method is applied, it can be placed at the left side of the scale of gravity. Therefore, a *general legal basis* suffices for the investigative method.

However, data protection regulations should already apply when personal information is *processed* by law enforcement authorities, and not just when personal information is *stored* in police systems. In its case law, the ECtHR often refers to a relatively old data protection treaty of the Council of Europe. Instead, the EU *data protection regulations* should be adopted by the ECtHR as a baseline of protection.[49] The legislation is already used by most law enforcement authorities within the EU and is applicable to the mere processing of personal information by law enforcement officials.

B Automated gathering of publicly available online information

A more serious privacy interference takes place in relation to the automated gathering of publicly available online information. The use of such a 'technically sophisticated system' and the fact that information is processed concerning individuals who are not suspected of a crime indicate that the ECtHR will at least require States to balance the privacy interests of the individuals involved with regard to the aim pursued by law enforcement authorities.

The result of that balancing test should be reflected in *detailed regulations in either statutory law or in public guidelines* issued by law enforcement authorities that restrict the automated gathering of publicly available online information. Data protection regulations can aid in creating those detailed regulations and determining adequate safeguards.

48 See also subsection 4.1.1 under A.

49 See Koops 2013, p. 662 for an extensive analysis of EU data protection regulations for law enforcement authorities with regard to the processing of publicly available online information.

C Observing online behaviours of individuals

The observation of online behaviours of individuals can likely be placed at the low end of the scale of gravity for privacy interferences, given that these behaviours can be observed by anyone. The ECtHR does not require detailed regulations in statutory law for the application of observation as an investigative method in the physical world. An important difference compared to its offline counterpart, is that during online observation, law enforcement officials can also quickly collect information regarding an individual's past behaviours. When information is collected from past behaviours, the investigative method of the manual gathering of publicly available online information is applicable. Online observation only concerns the monitoring of behaviours that start from a specific point in time.[50]

The gravity of the privacy interference that takes place when the investigative method is applied depends on the factors developed by the ECtHR in case law. The nature, scope, and duration of the investigative method will influence the gravity of the privacy interference. For example, a single observation of the online behaviours of individuals for a brief period is considered as a minor privacy interference.

With an increasing intensity of observation, the gravity of the interference and desirable quality of the law will change accordingly. Only detailed regulations for the investigative method can prescribe for law enforcement authorities to take account the factors provided above and articulate the grounds for ordering the measure and authorities that conduct the investigative method. Therefore, a *detailed legal basis in law in either statutory law or in public guidelines* is desirable for the investigative method.

4.2 Issuing data production orders to online service providers

This section analyses the gravity of the privacy interferences that take place when law enforcement officials collect information by issuing data production orders to online service providers.

Issuing a data production order to a telecommunication service provider is considered to be a similar investigative method to issuing such an order to an online service provider. Subsection 4.2.1 thus analyses case law with regard to telecommunication service providers. In subsection 4.2.2, data production orders that are issued to online service providers are further analysed in light of their interference with the right to privacy. Subsection 4.2.3 then concludes the section by determining which quality of the law is *desirable* for data production orders that are issued to online service providers.

50 See for a similar distinction CTIVD 2014, p. 9 and p. 42.

4.2.1 Privacy and data production orders issued to telecom providers

The ECtHR considers the registration and storage of the numbers dialled on a particular telephone and the time and duration of each call as an interference with the right to respect for private life and correspondence in art. 8(1) ECHR.[51]

In the case of *Malone v. The United Kingdom*, the ECtHR first noted that the records of metering information – in particular the numbers dialled on a telephone – are an integral part of communications.[52] Greer (1997, p. 12) explains that the practice of 'metering' consists of the recording of all numbers dialled from a particular telephone by the (U.K.) Post Office for U.K. law enforcement authorities. In the current study, such information is considered as 'traffic data'.

In case law, the ECtHR explicitly differentiates traffic data from content data. For instance, in the case of *P.G. and J.H. v. The United Kingdom*, the ECtHR noted that the data production orders issued to a telecommunication provider were strictly limited to numbers dialled from the suspect's flat between two specific dates.[53] The contents of communications can be understood as data with regard to the meaning or message conveyed by the communication, which is different from traffic data.[54] A more serious privacy interference takes place when law enforcement officials obtain content data.[55]

Gravity of the privacy interference

The above exaxmined case law indicates that the ECtHR does not regard the privacy interference that takes place when traffic data is collected as particularly serious. The privacy interference caused by the investigative method can be placed at the left side of the scale of gravity, indicating that between a minor interference with the right private life takes place.

Required quality of the law

In the case of *Malone v. The United Kingdom*, the ECtHR found that the domestic legislation with regard to the collection traffic data from telecommunication providers was not 'in accordance with the law', since no specific regulations were available concerning (1) the scope of the investigative method and (2) the manner in which the 'metering information could be obtained from telecommunications providers (cf. Greer 1997, p. 12).[56]

---

51 ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 84. See also ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 42.

52 ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 84.

53 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 46.

54 See the explanatory memorandum Convention on Cybercrime, par. 209. See also subsection 2.2.2 under B.

55 See also ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 46.

56 See ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 87.

Seventeen years later, the ECtHR found in the case of *P.G. and J.H. v. The United Kingdom* that the UK Telecommunications Act and Data Protection Act of 1984 contain an accessible and foreseeable statutory provision for law enforcement authorities to obtain billing information by issuing data production orders.[57] However, that legal basis only detailed the provision that processors of the traffic data were not liable when they disclosed information to law enforcement authorities in a criminal investigation (cf. Ölçer 2008, p. 294). The ECtHR was not persuaded by the defendant's argument that (more) detailed regulations were required for the investigative method.[58]

4.2.2 Privacy and data production orders issued to online service providers

This subsection examines the gravity of the privacy interferences that take place when data production orders are issued to online service providers. It is also considered whether the case law regarding the application of data production orders that are issued to telecommunications providers and the required quality of the law align with the examined digital investigative method. In chapter 2, data production orders that are issued to online service providers were distinguished in the following types of data: (A) subscriber data, (B) traffic data, (C) other data, and (D) content data.

As explained in subsection 2.2.1, this categorisation of data is partly derived from the categorisation made in the Convention on Cybercrime. States that have ratified this convention are obliged to introduce a differentiation in the legal protection of data production orders *"in accordance with its sensitivity"*.[59] According to the convention's explanatory memorandum, this implies that the substantive criteria and procedures that to apply the investigative power may vary according to the sensitivity of the data.[60]

Indeed, different types of data production orders issued to online service providers interfere with the right to privacy in different ways. These particular interferences with the right to privacy as articulated in art. 8 ECHR are further examined below.

A Subscriber data

The collection of subscriber information from online service providers by law enforcement officials interferes with the right to respect for private life. The reason is that the information is secretly gathered from online service providers and stored in police systems. The examined case law has shown that an interference takes place with the right to privacy when personal information from individuals is systematically gathered and stored in a police system.

57 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 45.
58 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 47.
59 Art. 15 Convention on Cybercrime.
60 Explanatory memorandum Convention on Cybercrime, par. 31.

Gravity of the privacy interference
Subscriber data consists of a limited set of information and does not reveal information about the communications themselves. For these reasons, the privacy interference of obtaining subscriber data is considered less serious than the privacy interferences involved when traffic and content data is obtained by using data production orders.[61]

Alignment with the existing required quality of the law
Based on the case law with regard to data production orders that are issued to telecommunication providers, the ECtHR requires an accessible and foreseeable legal basis for a data production order.[62] The case of *P.G. and J.H. v. The United Kingdom* does not indicate that particularly detailed regulations in statutory law or guidelines are required to obtain data from telecommunications by using data production orders.[63]

It may be added here that it follows from the examined case of *K.U. v. Finland* in section 3.1 of chapter 3 that States have the positive obligation to implement legislation that makes it possible to obtain identifiable data, i.e., subscriber data, from online service providers for the prevention of disorder and crime.[64] Following the decision of the *K.U. v. Finland* case, either detailed regulations in statutory law or a more general legal power that authorises law enforcement officials to obtain subscriber data from online service providers must therefore be available in the domestic regulations of contracting States of the ECHR.

B Traffic data
In the case of *P.G. and J.H. v. The United Kingdom,* the traffic data concerned the numbers that a suspect had dialled from his telephone during a specific period of time. According to present-day standards, the privacy interference that takes place when traffic data is obtained from online service providers may be considered as more serious than the fixed telephone situation as discussed in by the ECtHR in *P.G. and J.H. v. The United Kingdom*. The first reason is that traffic data today also encompasses *location data* (see B.1). The second is that *internet traffic data* consists of information other than traffic data concerning communication by telephone (see B.2). The gravity of the privacy interferences caused by data production orders with regard to these two types of data and their alignment with the required quality of the law are further examined below.

B.1 Location data
The following example illustrates the privacy interference that can take place when location data is obtained from a telecommunication service pro-

61 This will be further argued and illustrated in this subsection under B and D.
62 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 45.
63 See subsection 4.1.1
64 ECtHR 2 December 2008, *K.U. v. Finland*, appl. no. 2872/02.

vider and further processed for law enforcement purposes. In 2012, I sent a data access request to my own telecommunications provider in order to obtain access to information that the provider had stored for law enforcement purposes.[65] The information, which was provided to me in an Excel file,[66] included location data that depicted the location of the telephone antennae to which my mobile telephone (with internet access) had been connected. I plotted the location of the telephone antennas on a map using publicly available online tools in order to visualise what this data can reveal.[67] The location data was also combined with the time and date that the mobile phone had been connected to the antennae, which were all part of the provided traffic data. All of the data pertained to a timespan of three days.

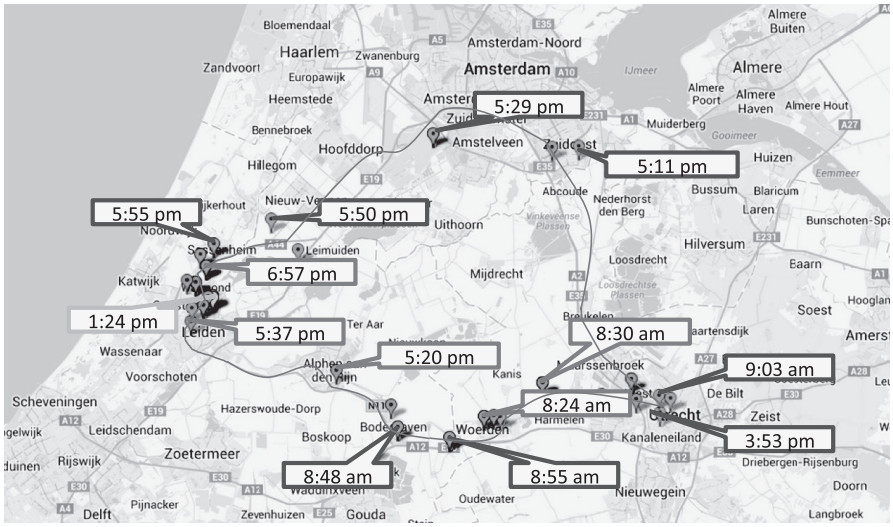

Figure 4.2: Representation of location data that can be derived from traffic data.

65 At the time, public telecommunication service providers were obliged by the Data retention act to retain traffic data relating to telephone data for 12 months and traffic data relating to internet data for 6 months. Subscribers have a right a right to access data under data protection regulations. I made use of this right. My data access request at my telecommunication provider aimed to find out what internet traffic data was retained by my telecommunications provider. See also J.J. Oerlemans, 'Leaving out notification requirements for data collection orders?', *LeidenLawBlog*, 17 October 2013. Available at: http://leidenlawblog.nl/articles/leaving-out-notification-requirements-for-data-collection-orders (last visited on 8 May 2014). The request was inspired by a German politician Malte Spitz, who also obtained access to his traffic data that was generated by mobile telephony. The politician used this information to illustrate the privacy infringement data retention obligations for telecommunication providers brings with (see 'Betrayed by our own data', *Die Zeit*, 26 March 2011. Available at: http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz (last visited 30 June 2014)).

66 The Excel file is available for review upon request at the author.

67 The provided location data was plotted on a map using the online service 'batchgeo'. Available at http://batchgeo.com/map/4db35deb53eb2727fb0f00b10e813087 (last visited on 25 June 2014).

Figure 4.2 clearly illustrates the insights into my private life that can be obtained using location data collected from my telecommunications provider. The dots on the map of Figure 4.2 illustrate the cell phone towers (32 in total) with which my mobile telephone was connected within the three-day period. The map also shows the time at which a connection was established between my telephone and the antenna on the cell phone tower. During those three days, I provided a cybercrime training course in the city of Utrecht. The map clearly shows how I took the train from Leiden Central Station to Utrecht Central Station and back. The thick line indicates the railroad track, which clearly runs between the dots that represent the cell phone antennae.

Gravity of the privacy interference

Figure 4.2 illustrates how location data can reveal an intricate picture of certain aspects of an individual's private life. With the information and a computer with an internet connection, a similar map can be created in 30 minutes. Thereby, an individual's movements can be made visible in a single glance. In addition, one can make an educated guess about this author's hometown by the number of dots around the city of Leiden on the map.

Telephone *traffic data* also consists of the calls made and received at specific times. Koops and Smits (2014, p. 141) point out that modern data processing techniques enable investigators to gain more insight into the personal lives of the involved individuals, even without taking notice of the 'contents' of information.[68] A detailed picture of certain aspects of an individual's private live can be obtained in particular when traffic data is collected over a longer period of time, combined with other information sources, and thoroughly analysed (cf. Koops & Smits 2014, p. 108-110).[69] These technological advancements must be taken into consideration when assessing the gravity of the privacy interference of investigative methods.

68 With reference to Hildebrandt & Gutwirth 2008 and Steenbruggen 2009, p. 56-57.

69 This observation is similar to the 'mosaic theory of privacy' that has been developed in the U.S. decision in the Maynard case (cf. Kerr 2013) (United States District of Columbia Circuit Court 6 August 2010, *United States v. Maynard*, 615 F.3d 544, (D.C. Cir. 2010). In the case of *Maynard*, a district court decided that the use of a GPS device to monitor the suspect's movements for a longer period of time amounted to a search that requires a warrant under the Fourth Amendment to the U.S. Constitution. Although the district court affirmed the U.S. doctrine that an individual's generally does not have reasonable expectation of privacy in public, the court found that the long-term observation of movements in the public amounts – taking in consideration the 'sum of its parts' – to a search that requires a warrant in the United States. Under the mosaic theory, a 'search' is perceived as a 'collective sequence of steps' rather than as individual steps (Kerr 2012, p. 313). As is illustrated in Figure 4.2, over time, the analysis of traffic information can reveal a 'mosaic of habits of an individual and relationships between individuals' (cf. Bellovin et al. 2014b, p. 556). Thus, the mosaic theory of privacy can help us understand how the analysis of traffic data – in particular location data – can seriously interfere with the right to respect for private life.

Alignment with existing required quality of the law

Considering the above analysis, it is clear that the processing of internet traffic data that has been obtained by data production orders issued to online service providers seriously interferes with the right to privacy. In the recent (2016) case of *Szabó and Vissy v. Hungary*, the ECtHR explicitly stated that "*the potential interferences with email, mobile phone and Internet services (…) attract the Convention protection of private life more acutely*".[70]

Given that greater privacy interferences takes place when traffic data is collected and processed by law enforcement officials today than in comparison to over than 15 years ago, it can be expected that more detailed regulations are now required for regulating data production orders. Existing ECHR requirements concerning traffic data obtained from telecommunications providers therefore misalign with the current reality of data production orders the regulations that follow from previous ECtHR case law with regard to data production orders issued to online service providers.

B.2 Internet traffic data

Internet traffic data consists of information other than telephone data. For example, it indicates at what time an internet connection is established and ended and which IP address the online service provider assigns to a device. This traffic data – which is also called 'session data' and 'logging data' – may be important for proving that a suspect used the Internet or a particular computer at a certain moment in time.[71]

Online service providers can also retain traffic information that reveals the 'destination IP address', which concerns the computer that an individual has connected with. That computer may be a server from an online service provider, such as an online storage provider, a social media service provider, or a webmail service provider. A destination IP address may therefore provide law enforcement officials with a lead to subsequently obtain private messages or other information from online service providers using data production orders.[72]

This analysis of the destination IP address also illustrates how difficult it can be to distinguish content data from traffic data. For instance, it is unclear whether (a) data with regard to search terms, (b) links to websites, (c) domain names, and (d) subject lines in private messages must be considered as content or traffic data (see Koops & Smits 2014, p. 93-106).[73] As a

70 ECtHR 12 January 2016, *Szabó and Vissy v. Hungary*, app. no 37138/14, § 53. It should be noted that it was also a factor that the investigative method involved the (potential) mass surveillance of telecommunications and not specifically a data production order to obtain traffic data from an online service provider. Nevertheless, the statement in my view indicates the collection of internet traffic data is deemed as privacy sensitive by the ECtHR.

71 See also subsection 2.2.2 under B.

72 How much information is available to law enforcement authorities depends on the type of service provider and the types of data that an online service provider retains.

73 With reference to Asscher & Ekker 2003, p. 104, Koops 2003, p. 77-78, Smits 2006, p. 416, Steenbruggen 2009, p. 56.

result, it is ambiguous whether these kinds of data are characterised as 'traffic data' or 'content data'. The collection and processing of (internet) traffic data clearly has the potential to seriously interfere with the right to respect for private life and correspondence as articulated as objects of protection in art. 8(1) ECHR.

Gravity of the privacy interference
Internet traffic information reveals at which point in time and for how long an individual made use of the Internet. The analysis in this subsection shows how traffic data and content data can be difficult to distinguish. Internet traffic data may indicate which websites an individual visited or which online services an individual used. The analysis of content data by law enforcement officials is a very serious interference with the right to respect to correspondence of individuals.

Alignment with the existing required quality of the law
As explained above with regard to the processing of location data, the ECtHR will consider the processing of internet traffic data as a serious interference with the right to privacy of individuals. It is expected the ECtHR will require detailed regulations for data production orders that are issued to obtain the data. In addition, the possibility that content data is obtained when these orders indicate that detailed regulations in statutory law is required for the investigative method.[74] Compared to the required quality of the law with regard to data production orders that are issued to telecommunication providers, a misalignment can be detected since the privacy interference is nowadays greater and more detailed regulations are expected to be required.

C Other data
The 'other data' category includes data that is not subscriber, traffic, or content data.[75] An example of this kind of data production order is the collection of profile information from online service providers, such as web forums or social media services.

An individual's online profile may, for instance, reveal that person's age, gender, interests, sexual orientation, and political affiliations. It may also include photographs that also reveal a person's race and possibly health conditions. The amount of information available depends on the amount of information an individual has disclosed to his social media provider on his private profile.[76]

74 See further under D.
75 See also subsection 2.2.2 under B.
76 If the information is publicly available, law enforcement officials can gather it and no data production orders are required.

Gravity of the privacy interference
The gathering and storage of personal information in the category of other data seriously interferes with the right to private life as defined in art. 8 ECHR. Profile information is, for instance, clearly more sensitive than subscriber information, due to the more sensitive type of information that often accompanies profile information and the potential variety of data. It can thus be argued that a serious privacy interference takes place when information from the 'other data' category is obtained from online service providers.

Alignment with the existing required quality of the law
Case law that deals with the collection of profile information using data production orders that are issued to online service providers is not available. However, the privacy interference that takes place appears to be more serious than the interference that results from collecting subscriber data. Since it is impossible to compare the privacy interference, and thus the required quality of the law, with the application of investigative methods that the ECtHR has decided on, a misalignment is clearly present.

D Content data
Content data can be defined as information that concerns the 'meaning or message' of communications.[77] In relation to online service providers, content data may take the form of private messages, including e-mails, which are sent between individuals who use a service; it may also include stored documents.[78] When content information is obtained from online service providers by the use of data production orders, there is no doubt that an interference takes place with the right to respect for private life and correspondence as protected by art. 8(1) ECHR.

Collecting private messages that are stored at online service providers can be compared with intercepting communications. In both cases, the meaning of messages in communications can be obtained. The ECtHR has made it clear in case law that the interception of telephone calls interferes with the right to respect for a person's private life and correspondence as protected in art. 8(1) ECHR.[79] As already mentioned in section 3.3, the ECtHR held in the case of *Copland v. The United Kingdom* that the interception of *electronic* communications concerning e-mail and information derived from the monitoring of personal internet usage also interferes with

77 Explanatory memorandum Convention on Cybercrime, par. 209. See also subsection 2.4.2.

78 Stored documents may be disclosed to law enforcement officials by cloud storage services, such as Google Drive of Microsoft's SkyDrive. See also subsection 2.2.2 under B.

79 See, e.g., ECtHR 6 September 1978, *Klass and Others v. Germany*, appl. no. 5029/71, § 41, ECtHR 24 April 1990, *Huvig v. France*, appl. no. 11105/84, § 25, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 42, ECtHR 18 February 2000, *Amann v. Switzerland*, appl. no. 27798/95, § 44 and ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 77.

the right to respect for private life and correspondence as protected in art. 8(1) ECHR.[80]

The collection of stored documents through data production orders is comparable to the search of an office or residence, during which law enforcement officials can seize documents (or a computer containing documents) for evidence-gathering purposes. The ECtHR considers a search in an office or residence undertaken by law enforcement authorities to be an interference with the right to respect for private life and a home as protected by art. 8(1) ECHR.[81] More recently, the ECtHR also specifically dealt with a situation in which law enforcement officials searched an office in order to seize computers and search documents stored therein for evidence-gathering purposes. As explained in subsection 2.4.2, in this study, this investigative method is called a 'computer search'. In case law involving computer searches, the ECtHR also found that the evidence-gathering activities interfered with both the right to home and correspondence as protected by art. 8(1) ECHR.[82] It can therefore be argued that the collection of *remotely* stored documents at online service providers interferes with the right to respect for home and correspondence as articulated as objects of protection under art. 8 ECHR (cf. Koops & Smit 2014, p. 141).[83]

Gravity of the privacy interference

The privacy interference that takes place when a data production order is issued to an online service provider to obtain content data is comparable to the privacy interference that occurs when electronic communications are intercepted. The reason is that in both cases, law enforcement officials secretly obtain information relating to the meaning or message of communications between individuals. The ECtHR regards the interception of communications as a serious privacy interference.[84] It requires detailed regulations with procedural safeguards for using the interception of communications as

80 See ECtHR 3 April 2007, *Copland v. The United Kingdom*, appl. no. 62617/00, §41-42.

81 See, e.g., ECtHR 26 December 1992, *Niemietz v. Germany*, appl. no. 13710/88, § 26, ECtHR 25 February 1993, *Funke v. France*, appl. no. 10828/84, § 48.

82 See ECtHR 27 September 2005, *Petri Sallinen and Others v. Finland*, appl. no. 50882/99, § 71, ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, appl. no. 74336/01, § 45, and ECtHR 14 March 2013, *Bernh Larsen Holding AS and Others v. Norway*, appl. no. 24117/08, § 105.

83 Note that the ECtHR interprets the concept of a "home" broadly (cf. Krabbe in: Harteveld 2004, p. 156). The term 'home' can also extent to certain professional or business premises. See, e.g., ECtHR 26 December 1992, *Niemietz v. Germany*, appl. no. 13710/88, § 30, ECtHR 27 September 2005, *Petri Sallinen and Others v. Finland*, appl. no. 50882/99, § 70, and ECtHR 14 March 2013, *Bernh Larsen Holding AS and Others v. Norway*, appl. no. 24117/08, § 104.

84 See, e.g., ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 67, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 46 and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 229.

an investigative method, in order to protect the individuals involved from arbitrary governmental interferences.[85]

The ECtHR requires the following procedures to be in place when (electronic) communications are intercepted: (1) the nature of the offences which may give rise to an interception order must be detailed; (2) a definition of the categories of people liable to have their telephones tapped must be available; (3) a restriction on the duration of telephone tapping must be set; (4) the procedure to be followed for examining, using, storing, and deleting the data obtained must be available; and (5) the precautions to be taken when communicating the data to other parties must be specified in the domestic legislation of a contracting State to the ECHR.[86] In the context of secret surveillance measures that involve the interception of communications, the ECtHR also considers it important that (6) the investigative method or surveillance measure is authorised by an independent authority, preferably a judge.[87]

With regard to computer searches, the ECtHR required in case law that detailed regulations with adequate procedural safeguards against abuse are available in the domestic laws of contracting States. For example, in the case of *Wieser and Bicos Beteiligungen GmbH v. Austria*, a law firm was searched and computers containing privileged documents were seized.[88] Here the ECtHR noted that it required in comparable cases that (1) the search was based on both a warrant issued by a judge and reasonable suspicion, (2) the scope of the warrant was reasonably limited, and – since the search took place in a lawyer's office – (3) the search is carried out in the presence of an independent observer to ensure that materials subject to professional secrecy were not removed.[89] In the case of *Wieser and Bicos Beteiligungen GmbH v. Austria*, the law enforcement officials did not follow the domestic procedures for computer searches.[90] The search was considered disproportionate and in violation of art. 8 ECHR, even though the domestic regulations were 'in accordance with the law'.

85 See, e.g., ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 67, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 46 and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 229.

86 See ECtHR 24 April 1990, *Huvig v. France*, appl. no. 11105/84, § 34, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 46, ECtHR 18 February 2000, *Amann v.* Switzerland, appl. no. 27798/95, § 76, ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 95 and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 231.

87 See most notably ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 257-267 with reference to ECtHR 26 April, *Dumitru Popescu v. Romania* (no. 2), appl. no. 71525/01, § 71.

88 ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, appl. no. 74336/01, § 8-10.

89 ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, appl. no. 74336/01, § 57.

90 ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, appl. no. 74336/01, § 63.

Alignment with the existing required quality of the law
The collection of stored private messages and stored documents from online service providers has been compared with case law regarding the interception of communications and computer searches. However, it is not clear whether the ECtHR also deems these investigative methods comparable with the collection of content data from online service providers. In my view, the seriousness of the privacy interferences and required quality of the law that can be deduced from this case law are also relevant for digital investigative methods. Case law with regard to the interception of communications and computer searches can therefore provide a good basis for regulating the examined digital investigative method.

4.2.3 Desired quality of the law

This subsection determines the *desirable* quality of the law based on the gravity of the privacy interference that takes place when data production orders are issued to online service providers.

In general, it should be observed that the gravity of the privacy interference that takes place when law enforcement officials obtain data from online service providers depends on the kind of data that is collected. It is also important to keep in mind that law enforcement authorities have the ability to obtain and combine different types of data. For instance, they may be able to collect financial data and internet traffic data from different online service providers and subsequently analyse that data in order to identify other individuals who may be relevant in a criminal investigation. It should be recalled here that the ECtHR considers the further processing of personal information as an increased interference with the right to privacy as defined in art. 8 ECHR. This factor should be taken into consideration when determining the desirable quality of the law.

The quality of the law that I view as desirable for regulating data production orders that are issued to online service providers is presented below. The four types of data are discussed separately.

A Subscriber data
With regard to subscriber data, the ECtHR likely does *not* regard the privacy interference as *particularly serious*. The first reason is that subscriber data consists of a limited set of data. The second is that subscriber data that is obtained from online service providers is not significantly different from subscriber data from telecommunication providers.

However, the desirable quality of the law should consist of *detailed regulations in statutory law* that stipulate under which conditions subscriber data can be obtained. A general legal basis in my view does not suffice, since the investigative method should be seen in connection with other (more intrusive) data production orders. This category of data should also be included in the detailed regulations for the investigative method.

B Traffic data

The collection of traffic data *seriously interferes* with the right to privacy of the individuals involved. Case law with regard to data production orders to obtain traffic data seems outdated. We no longer exclusively have telephone conversations using landlines. In addition, traffic data no longer only consists of the calls made and received coupled with date and time stamps. Today law enforcement officials can also collect location and internet-related traffic data from telecommunication providers, which can then be further processed to obtain a detailed picture of certain aspects of an individual's private life.

I therefore argue that *detailed regulations in statutory law* are desirable for the investigative method. The information is more intrusive than subscriber data, since traffic data consists of a broader category of data and is more sensitive in nature than subscriber data. As a procedural safeguard, I find the *authorisation of an investigative judge* desirable.

C Other data

The collection of other data through data production orders *seriously interferes* in the right to privacy of the individuals involved. Law enforcement officials are able to collect many different types of potentially sensitive data from online service providers, such as profile information from social media services. It is often unclear from the outset how much and what kind of information is going to be obtained.

Taking into account present-day standards, I argue it is desirable to implement *detailed regulations in statutory law* for the investigative method. As a procedural safeguard, the *authorisation of a higher authority* (such as a public prosecutor) is also desirable. Since the information can also encompass photographs of individuals who are attached to a (private) profile, *the authorisation of an investigative judge* is in my view also appropriate.

D Content data

When private messages are obtained, the collection of content data *seriously interferes* with the right to respect for private life and correspondence. The collection of content data can also interfere with the right to respect for home and correspondence when stored documents are gathered.

In my view, a *detailed legal basis in statutory law* is desirable for data production orders relating to content data. In addition, the *authorisation of an investigative judge* is in my view appropriate. That means that typically the request for a warrant to obtain the data is also restricted. For private messages, that restriction can be set by making it mandatory for data production orders to specify the relevant time period. For stored documents, filters from forensic software can be utilised to select the relevant documents for law enforcement authorities.

4.3 Applying online undercover investigative methods

This section analyses the gravity of the privacy interferences that take place when online undercover investigative methods are applied. The ECtHR has only developed case law with regard to the application of undercover investigative methods in the physical world. The application of undercover investigative methods on the Internet may or may not interfere with the right to privacy in a different manner.

To answer that question, the case law with regard to the application of undercover investigative methods in the physical world is first examined in subsection 4.3.1. Subsection 4.3.2 then examines the privacy interferences that take place when the digital counterparts of these methods are applied. Subsection 4.3.3 subsequently concludes the section by determining the *desirable* quality of the law for regulating undercover investigative methods.

4.3.1 The right to privacy and undercover investigative methods

In its case law regarding undercover investigative methods, the ECtHR usually determines whether an undercover investigative method interferes with the right to a fair trial, as defined in art. 6 ECHR.[91] Krabbe (in: Harteveld 2004, p. 144) explains this by arguing that the ECtHR often first considers art. 6 ECHR in cases where an applicant has protested against the legitimacy of an undercover operation. After the test with regard to art. 6 ECHR is conducted, the ECtHR does not consider it necessary to also test the legitimacy of the undercover operation under art. 8 ECHR.[92]

Case law of the ECtHR with regard to undercover operations and the right to privacy as articulated in art. 8 ECHR is scarce. The case of *Lüdi v. Switzerland* is an exception.[93] Here the ECtHR did consider whether interference with the right to privacy took place in the context of an undercover operation. In this case, an undercover agent bought drugs from Mr Lüdi as part of a 'pseudo-purchase' investigative method.[94] The facts are as follows. A Swiss law enforcement officer went undercover using the assumed name of 'Toni' and pretended to be a potential buyer of cocaine that was presumably being sold by Mr Lüdi. After meeting with Mr Lüdi three times, (undercover agent) Toni reported that Mr Lüdi had promised to sell him, as an intermediary, two kilograms of cocaine worth 200,000 Swiss francs.

91 See, e.g., ECtHR 9 June 1998, *Teixeira de Castro v. Portugal*, no. 44/1997/828/1034, ECtHR 5 February 2008, *Ramanauskas v. Lithuania*, appl. no. 74420/01 and ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06.

92 Krabbe in: Harteveld 2004, p. 144, referring to ECtHR 12 July 1988, *Schenk v. Switzerland*, appl. no. 10862/84.

93 See ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86.

94 See ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86, § 9-13.

The suspect had also borrowed 22,000 Swiss francs from a third person for the purchase of cocaine or other narcotics. After arresting the suspect, the Swiss police searched his home and found traces of cocaine and hashish on a number of objects.[95]

With regard to the legitimacy of the undercover operation, the ECtHR found that no interference took place with the right to respect for private life. It reasoned that: *"Mr Lüdi must (…) have been aware from then on that he was engaged in a criminal act punishable under Article 19 of the Drugs Law and that consequently he was running the risk of encountering an undercover police officer whose task would in fact be to expose him."*[96] In other words, in the *Lüdi* case, the ECtHR seems to have adopted the approach that individuals who engage in criminal activities do not have a reasonable expectation of privacy, because they should be aware that undercover investigative methods could be used against them (cf. Ölçer 2008, p. 279). This would be a far-reaching approach, since it denies individuals involved in undercover operations from protection by art. 8 ECHR.[97] This aspect of the *Lüdi* case is critically analysed in subsection 4.3.3.

Gravity of the privacy interference

Since no other case law is available with regard to the privacy interference that takes place when undercover investigative methods are applied, it is not possible to determine the gravity of the privacy interference.

However, as mentioned in the introduction to this section, the ECtHR does test whether undercover investigative methods comply with the right to a fair trial. More specially, the ECtHR tests whether no entrapment has taken place. In the case of *Teixeira de Castro v. Portugal*, the ECtHR held that the right to a fair trial would be violated when law enforcement officials *"do not confine themselves to investigating criminal activity in an essentially passive manner, but exercise an influence such as to incite the commission of the offense"*.[98] Essentially, the ECtHR tests whether the offence would have been committed without the intervention of law enforcement authorities (cf. Ölçer

95 See ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86, § 14.

96 ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86, § 40-41. Note that the ECtHR does consider it an interference with the right to respect for correspondence as provided in art. 8 ECHR, from the point that law enforcement official records a conversation with the suspect during a criminal investigation. See, e.g., ECtHR 12 May 2000, *Khan v. the United Kingdom*, appl. no. 35394/97, § 26-28, ECtHR 8 April 2003, *M.M. v. the Netherlands*, no. 39339/98, § 29 and 79 and ECtHR 10 March 2009, *Bykov v. Russia*, appl. no. 4378/02, § 72.

97 The ECtHR may have been inspired by the U.S. doctrine on a 'reasonable expectation of privacy' in undercover operations. See subsection 9.4.2 for further analysis.

98 See ECtHR 9 June 1998, *Teixeira de Castro v. Portugal*, no. 44/1997/828/1034, § 38.

2014, p. 16). An undercover operation should remain 'essentially passive'.[99] Importantly, the ECtHR has articulated qualitative requirements for the domestic legal frameworks of contracting States to prevent entrapment from occurring and to ensure a fair trial.[100] These requirements are such that it is possible to transpose them to requirements for the *regulation* of undercover operations. Thus, although these requirements are based in art. 6 ECHR, they, or aspects of them, are similar to requirements that apply to interferences in the context of art. 8 ECHR. As such, it is taken as a point of departure in this study that the art. 6 ECHR may be equated with art. 8 ECHR requirements. The qualitative requirements that affect the regulation of undercover investigative methods themselves are further examined below.

Required quality of the law

In relation to the regulation of undercover investigative methods, it is important to note that the ECtHR required in the case of *Furcht v. Germany*: *"clear and foreseeable procedures for authorising investigative measures, as well as for their proper supervision"*.[101] The ECtHR thus requires (1) detailed regulations for undercover investigative methods and (2) the procedural safeguard of supervision for undercover investigative methods.

In addition, the ECtHR has repeatedly emphasised in case law that an investigative judge provides 'the most appropriate means' for supervising undercover operations.[102] Nevertheless, the ECtHR also accepts the supervision of a public prosecutor, insofar 'adequate procedures and safeguards' are available.[103] It does not concretely explain which procedures and safeguards are considered adequate. However, it is clear that the procedures for undercover operations must ensure transparency regarding the operations themselves and aim to prevent entrapment by law enforcement authorities.

---

99 See ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, §47. See also ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09 § 51. To determine whether law enforcement authorities interfered in an active manner that brought the suspect to committing the offence, the ECtHR takes into consideration the following four factors: (1) the reasons underlying the undercover operation; (2) the behaviour of the law enforcement authorities; (3) the existence of a reasonable suspicion that the suspect was involved in criminal behaviours; and (4) the predisposition to the crime of a suspect (see Ölçer 2014, p. 16, see also ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, *EHRC* 2011/9, m.nt. Ölçer).

100 See ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, § 48. In the case of *Bannikova v. Russia*, the ECtHR also noted that the need for transparency generally requires that undercover agents and other witnesses can be heard in court and be cross-examined by the defence, unless detailed reasons are provided for denying this right to questioning (ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, § 65).

101 ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09, § 53.

102 See 50 ECtHR 24 June 2008, *Milinienè v. Lithuania*, appl. no. 74355/01, § 39: *"Moreover it had been adequately supervised by the prosecution, even if court supervision would have been more appropriate for such a veiled system of investigation"*. See also ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, § and ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09, *EHRC* 2015/1, m. nt. Ölçer at 9.

103 ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, §50.

4.3.2 The right to privacy and online undercover investigative methods

This subsection examines the gravity of the privacy interferences that take place when undercover investigative methods are applied in an online context. It is also consided whether the case law regarding the application of undercover investigative methods in the physical world and required quality of the law align with the law that is required for the examined online application of the investigative method.

In chapter 2, online undercover investigative methods were categorised as: (A) online pseudo-purchases, (B) online undercover interactions with individuals, and (C) online infiltration operations. These three digital investigative methods are further examined below.

A Online pseudo-purchases

An online pseudo-purchase is an investigative method in which an undercover law enforcement official purchases a good or data that a suspect is offering on the Internet (e.g., in an online forum), in order to collect evidence in a criminal investigation or with the intention to arrest an individual upon delivery of the good or data.[104]

Gravity of the privacy interference

The case of *Lüdi v. Switzerland* indicates that the ECtHR does not consider the purchase of drugs offered by suspects as a privacy infringing activity.[105] However, as the analysis in subsection 4.3.1 has shown, the ECtHR does test whether the right to a fair trial as defined in art. 6 ECHR is violated in such situations. In particular, the ECtHR tests whether entrapment took place. The procedures and safeguards required to ensure a fair trial in connection with undercover investigative methods used in the physical world also apply in an online context, since the risk of entrapment exists here as well.

When a law enforcement official purchases a good or data from an individual in an online forum, that good or data is already being offered on the Internet to anyone who wants to purchase it. In such a situation, the risk of entrapment is small. It may also be argued that a minor privacy interference is taking place. The individual offering the good or data may feel betrayed after a transaction with a law enforcement official has been completed. However, the privacy interference remains limited due to the one-time application of the investigative method.

When the physical and online pseudo-purchase are compared, the major differences are that the online pseudo-purchases can be applied *anywhere in the world* and that both the buyer and the seller can (attempt to) remain *anonymous*. The latter can be done by using a nickname and avoiding reg-

104 See also subsection 2.2.2 under C.

105 ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86, §40-41. See also, e.g., ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06 and ECtHR 5 February 2008, *Ramanauskas v. Lithuania*, appl. no. 74420/01.

istration of the originating (public) IP address at the platform that provides the service. In addition, both the seller and the buyer can make use of webmail services that are offered through Tor, which help to hide the originating (public) IP address. In my view, online pseudo-purchases' two characteristics of (1) global reach and (2) anonymity do not significantly influence the intrusiveness of the digital investigative method of an online pseudo-purchase.[106]

Alignment with the existing required quality of the law
The above analysis indicates that the privacy interference that takes place when online pseudo-purchases are performed is non-existent from the perspective of the ECtHR. The risk of entrapment does exist in an online context, as it does in a physical world pseudo-purchase. However, in my view the risk is not greater in an online context. The detailed procedures and safeguards necessary to ensure a fair trial when this undercover investigative method is used in the physical world therefore align well with the application and required quality of the law when it is used in an online context.

B Online undercover interactions with individuals
Online undercover interactions with individuals to gather evidence as part of criminal investigations can take place on many internet platforms, such as chat services, online black markets, and social media services. With the right knowledge of internet subcultures, law enforcement officials can interact and build relationships with individuals under a credible, fake identity in order to gather evidence (cf. Siemerink 2000b, p. 145).[107] It is straightforward for undercover agents to create an 'online identity' (cf. Siemerink 2000b, p. 143). Law enforcement authorities can even prepare for online undercover investigations by creating many online identities – complete with pre-set profiles on social media websites – that can be used later in time. Due to the lack of physical proximity to the individual involved in the operation, an undercover agent is in no immediate risk of bodily injury if his cover is exposed (cf. Siemerink (2000b, p. 144).[108] Another interesting aspect of online undercover interactions as an investigative method is that law enforcement officials may be able to take over an account that is voluntarily provided by an individual who has either already interacted with suspects or has an interesting information position and cooperates with law enforcement authorities as an informant.[109] The gravity of the privacy interference that takes place in relation to this investigative method is considered below.

106 These characteristics do pose questions with regard to the territorial limitation of enforcement jurisdiction. These questions are addressed in section 9.4.
107 See also subsection 2.2.2 under C.
108 That is not to say that undercover law enforcement officials or informant are never subjected to a risk of bodily injury after an online undercover operation. Criminals may seek out an online undercover agent in order to punish that individual in the physical world.
109 See also subsection 2.2.2 under C.

Gravity of the privacy interference
Online undercover interactions can take place with individuals anywhere in the world and both participants – namely the undercover agent and the involved individual – can stay relatively anonymous. The individual who is targeted by the undercover operation cannot interpret certain communication signals (e.g., non-verbal[110] signals).

However, compared to undercover interactions with individuals in the physical world, online undercover investigative methods do not interfere more seriously in the private lives of the individuals involved. In the case of undercover interactions with individuals both in 'cyberspace' and 'meatspace',[111] undercover agents often gain the trust of individuals involved in the criminal investigation and develop personal relationships. When law enforcement officials mislead suspects in an undercover operation, those individuals will often feel betrayed after the operation (cf. Kruisbergen & De Jong 2010, p. 218). A privacy interference clearly takes place, given that personal relationships may be developed with the individual involved in this type of undercover operation. The privacy interference may be regarded as being greater than in an (online) pseudo-purchase, since the investigative method involves more than a one-time application.

Alignment with existing quality of the law
The individuals involved in online undercover interactions must be protected from an arbitrary governmental application of power and a mechanism must be in place to ensure that no entrapment by law enforcement officials takes place. During these online interactions with individuals, the same risk of entrapment arises as when the interactions take place in the physical world. In both cases, law enforcement officials must remain 'essentially passive' in the operation. The required existing quality of the law in the form of detailed regulations for the undercover investigative methods and articulated safeguards by the ECtHR with regard to the supervision of undercover operations (preferably by an investigative judge) therefore align well for application to the investigative method in an online context, in as far as entrapment may become an issue in the course of such operations.

C Online infiltration operations
Infiltration operations are similar to undercover interactions with individuals. The distinction is that the former includes the possibility that law enforcement officials can commit (authorised) crimes in order to maintain their cover and gain the trust of the targeted individuals in a criminal investigation (cf. Joh 2009, p. 166). In other words, in infiltration operations, law enforcement officials can *participate* in crime with other individuals in order

110 Obviously, 'verbal' is in this context interpreted as written text.
111 See for this comparison between cyberspace and meatspace, e.g., https://en.wikipedia.org/wiki/Real_life#Related_terminology (last visited 18 December 2015).

to gather evidence and gain access to that organisation's upper echelons (cf. Joh 2009, p. 167).[112]

Gravity of the privacy interference
The gravity of the privacy interference that takes place in online infiltration operations is similar to that of the investigative method of online interactions with individuals. However, in online infiltration operations, risks that endanger the *integrity* of criminal investigations are greater. A specific risk of infiltration operations is that undercover agents can 'go rogue' and commit unauthorised crimes, especially when civilians are used as undercover agents (cf. Kruisbergen & De Jong 2010, p. 130-131).[113] Law enforcement officials can also overstep their mandate and engage in unauthorised illegal activities.[114] The risk of entrapment is greater in the context of infiltration operations than in undercover interactions.

Alignment with the existing required quality of the law
Online infiltration operations can be characterised by their global reach and the possibility to participate in a criminal investigation while remaining relatively anonymous. The privacy interference that takes place in online infiltration operations is similar to that of the investigative method of online interactions with individuals and does not appear different to infiltration operations in the physical world. In online infiltration operations, the risks that endanger the integrity of criminal investigations and of entrapment are clearly present. In online infiltration operations, governmental agents or civilians are authorised to participate in a criminal organisation, which creates the risk that they will overstep their mandate. The required quality of the law in the form of detailed regulations for the investigative method and proper supervision, preferably by an investigative judge, therefore aligns well with the quality of the law for online infiltration operations.

4.3.3 Desired quality of the law

This subsection determines the *desirable* quality of the law based on the gravity of the privacy interference that takes place when online undercover investigative methods are applied.

First, a general comment must be made regarding the lack of case law for undercover investigative methods as they relate to art. 8 ECHR. As the analysis in subsection 4.3.1 has shown, the ECtHR indicated in the case of

112 See also subsection 2.2.2 under C.

113 This research is restricted to investigative methods that are applied by law enforcement officials. Therefore, this aspect is not elaborated upon in this study.

114 For example, in the Silk Road investigation (also described in subsection 2.3.3), an undercover law enforcement agent transferred bitcoins (a virtual currency) to himself without authorisation. See Reuters, 'US undercover agent jailed for six years for Silk Road Bitcoin theft', *BBC News*, 20 October 2015. Available at: http://www.bbc.com/news/business-34588568 (last visited on 12 May 2016).

Lüdi v. Switzerland that individuals do not have a reasonable expectation of privacy when a pseudo-purchase is applied as an investigative method. Therefore, for that undercover investigative method, no interference with the right to privacy as defined in art. 8 ECHR takes place. I disagree with that decision, as fundamental rights apply to anyone. From a principled viewpoint, it is does not make sense to exclude individuals subjected to undercover operations from protection against arbitrary governmental interferences. The protection of all individuals from the arbitrary use of governmental power is an essential component of the rule of law and human rights (cf. Joubert 1994, p. 21 and Corstens 1995, p. 547-548). Furthermore, as part of the presumption of innocence, law enforcement officials cannot decide in advance whether a person is a criminal and should be excluded from protection under art. 8 ECHR (cf. Joubert 1994, p. 21). It is unclear whether the ECtHR would repeat the reasonable expectation of privacy doctrine as developed in the *Lüdi* case today. In the more than 20 years that have followed the decision of *Lüdi*, the ECtHR has not again excluded the privacy interests of individuals in the context of undercover operations (cf. Krabbe in: Harteveld 2004, p. 153).[115] Since this case, the ECtHR has repeatedly dealt with the legitimacy of undercover investigative methods. Nonetheless, in these subsequent cases the ECtHR has focused on the right to a fair trial and the question of whether entrapment has taken place. In those cases, the ECtHR required detailed regulations with safeguards to ensure a fair trial and prevent entrapment by law enforcement officials. As explained above, the point of departure is that those requirements are similar to those set for interferences with privacy in the context of art. 8 ECHR.

Second, it is important to note that the analysis in subsection 4.3.2 has shown that although online undercover investigative methods are similar to their non-digital counterparts, they are not the same as undercover investigative methods in the physical world. They are different in the sense that online undercover operations have a global reach and can be conducted with the relative anonymity that the Internet offers to everyone. The opportunity to 'take over an account' of an individual who is already part of a criminal organisation or has a particular information position is unique to online undercover investigative methods. Nevertheless, when undercover investigative methods are applied in an online context, in my view the gravity of the interference to the right to privacy is not notably different from when they are applied in the physical world. Thus, whilst differences between digital and non-digital variants may have (more) bearing on issues

115 With the exception of the case of ECtHR 10 March 2009, *Bykov v. Russia*, appl. no. 4378/02, § 72, in which an undercover agent recorded a conversation with the suspect. In this case, the recording of the conversation with an undercover agent led to an interference with the right for private life under art. 8 ECHR. However, the privacy interference thus focused on the private recording, not the undercover interactions with the individual himself.

of misalignment in the context of other norms (such as that concerning entrapment in art. 6 ECHR), they are not substantial from the perspective of art. 8 ECHR.

The quality of the law that is in my view desirable for the regulation of the three identified online undercover investigative methods is presented below.

A Online pseudo-purchases

The gravity of the privacy interference that takes place when an online pseudo-purchase is applied is limited, due to the one-time application of the investigative method. However, the risk of entrapment is still present. The *detailed regulations in statutory law* that are already required by the ECtHR for undercover investigative methods are also desirable for the regulation of online pseudo-purchases as an investigative method. The ECtHR regards the involvement of an investigative judge as 'the most appropriate means' for supervising an undercover operation. However, considering the minor privacy interference and the entrapment risk involved, my view is that *the involvement of a public prosecutor* in supervising the application of this online undercover investigative method is appropriate and desirable.

B Online undercover interactions with individuals

The gravity of the privacy interference is greater when online undercover interactions with individuals are applied as an investigative method than when online pseudo-purchases are used. Law enforcement officials obtain more detailed knowledge about aspects of the private life of the individuals involved and the investigative method is applied for a longer period of time. The risk of entrapment can also be present when this digital investigative method is applied.

Therefore, I argue that both (1) a *detailed legal basis in statutory law* for the investigative method and (2) the *supervision of an investigative judge* as a procedural safeguard are desirable for regulating the investigative method.

C Online infiltration operations

The gravity of the privacy interference in the context of online infiltration operations is similar to when the investigative method of online undercover interactions is applied. However, the safeguards to prevent entrapment and help ensure transparency may be of greater importance in online infiltration operations. The reason is that in online infiltration operations, risks that endanger the *integrity* of criminal investigations and entrapment are more frequently present (cf. Ölçer 2014, p. 18). The quality of the law that is desirable consists of (1) a *detailed legal basis in statutory law* to apply to the investigative method and (2) the procedural safeguard of *an investigative judge* to supervise the online undercover investigative method.

4.4 Performing hacking as an investigative method

This section analyses the privacy interferences that take place when hacking is applied as an investigative method. As the ECtHR has not developed case law addressing this situation, an analogy with other investigative methods must be made.

The investigative methods of network and remote searches are comparable with the investigative method of a computer search. The case law concerning computer searches and the right to privacy is examined in subsection 4.4.1. The investigative method of using policeware is comparable with investigative methods involving the interception of electronic communications, more specifically using 'covert listening devices'. The case law with regard to the use of covert listening devices and the right to privacy is examined in subsection 4.4.2. In subsection 4.4.3, the privacy interferences that take place when hacking is performed as an investigative method are examined. Subsection 4.4.4 concludes the section by determining the *desirable* quality of the law for the regulation of hacking as an investigative method.

4.4.1 The right to privacy and computer searches

The gravity of the privacy interference that takes place in relation to computer searches is explored in this subsection by examining the relevant case law of the ECtHR. The investigative method is visualised in Figure 4.3.

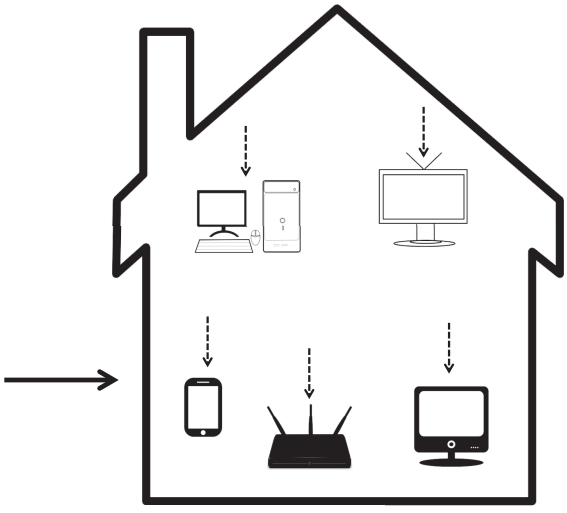

Figure 4.3: Simplified model of a computer search.

Figure 4.3 illustrates how a search can be conducted at a certain place, such as residence. During the search, law enforcement officials can subsequently seize (all types of) computers that may contain evidence that is relevant to

the criminal investigation. Figure 4.3 is called a simplified model of a computer search, because the initial search can also take place at any different place.

Gravity of the privacy interference

In the early 1990s, the ECtHR indicated in case law that a search in an office or residence by law enforcement officials is considered a serious interference with the right to respect for private life and home as protected by art. 8(1) ECHR.[116] In these cases, the concept of 'home' is interpreted broadly and the ECtHR has clarified that it can also encompass business premises.[117] Hacking as an investigative method and a search inside a residence are comparable as investigative methods, given that both involve an activity in which law enforcement officials gain access to a private place and can thereafter obtain intimate knowledge about individuals' private lives. Personal information such as documents, photos, and videos are now often stored digitally on computers instead of in physical boxes that are kept in certain places. When they use a search as an investigative method, law enforcement officials can gain access to a place and then seize items of interest – such as computers – for later analysis.

The ECtHR has recently started interpreting the right to privacy with regard to computer searches, i.e., when the search of a place results in computers being seized.[118] For example, in the case of *Prezhdarovi v. Bulgaria*, the individuals involved were suspected of using unlicensed software. Their computers were set up in a garage as part of a computer club.[119] In this case, the Bulgarian police conducted a search of the residence's garage without a judicial warrant. During this search, they seized computers that contained letters and other personal information about friends and clients of the suspects.[120] The ECtHR considered these investigative activities as an interference with the right to privacy as defined in art. 8 ECHR. In other case law with regard to computer searches, the ECtHR has explicitly noted that the search of a place and the seizure of computers amount to an interference with the right to respect for home and correspondence.[121] These interfer-

116 See, e.g., ECtHR 26 December 1992, *Niemietz v. Germany*, appl. no. 13710/88, § 26, ECtHR 25 February 1993, *Funke v. France*, appl. no. 10828/84, § 48.

117 See subsection 3.3.2.

118 See ECtHR 27 September 2005, *Petri Sallinen and Others v. Finland*, appl. no. 50882/99, § 71, ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria,* appl. no. 74336/01, § 45, ECtHR 3 July 2012, *Robathin v. Austria*, appl. no. 30457/06, § 51, ECtHR 14 March 2013, *Bernh Larsen Holding AS and Others v. Norway*, appl. no. 24117/08, § 105 and ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 41.

119 ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 12.

120 ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 21.

121 See, e.g., ECtHR 27 September 2005, *Petri Sallinen and Others v. Finland*, appl. no. 50882/99, ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria,* appl. no. 74336/01, ECtHR 3 July 2012, *Robathin v. Austria*, appl. no. 30457/06, ECtHR 14 March 2013, *Bernh Larsen Holding AS and Others v. Norway*, appl. no. 24117/08 and ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05.

ences with the right to privacy can be considered as serious; more serious than, for instance, the surveillance by law enforcement officials of an individual in public. Considering the gravity of the privacy interference, more detailed regulations with specific procedural safeguards will be required for this investigative method. The required quality of the law for computer searches is further examined below.

Required quality of the law
It is emphasised here that the privacy interference that takes place when computers are seized and analysed is serious due to the large amounts of information that are nowadays stored on computers (cf. Groothuis & De Jong 2010, p. 280 and Conings & Oerlemans 2013, p. 26). The ECtHR requires the following quality of the law for computer searches.

In case law with regard to computer searches, the ECtHR has clarified that it strongly prefers the involvement of an investigative judge. For instance, in the case of *Prezhdarovi v. Bulgaria*, the court found it especially important that adequate judicial review was not available. Nevertheless, in the words of the ECtHR: *"the absence of a prior judicial warrant may be counterbalanced by the availability of a retrospective judicial review"*.[122] In *Prezhdarovi v. Bulgaria*, the ECtHR also pointed out that the scope of a search-and-seizure operation should be limited to relevant information.[123]

When evaluating the case law with regard to computer searches, in my view the essential safeguard that the ECtHR requires is a *"meaningful judicial scrutiny of the search and seizure"* of computers.[124] This safeguard can be interpreted as a requirement for authorisation of an investigative judge that is limited in scope to relevant information.

4.4.2 The right to privacy and the use of covert listening devices

The ECtHR has also made it clear in case law that using covert listening devices to intercept private communications amounts to an interference with the right to respect for private life.[125]

Gravity of the privacy interference
The ECtHR regards the privacy interference that takes place when covert listening devices are used as serious, similar to the privacy interference that takes place when communications are obtained through the interception of

122 ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 46. The ECtHR also noted in the case of *Petri Sallinen* (§ 89) that it was *"struck by the fact that there was no independent or judicial supervision."*

123 See ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 49. See also, e.g., ECtHR 3 July 2012, *Robathin v. Austria*, appl. no. 30457/06, § 48.

124 ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 50.

125 See, e.g., ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 25, ECtHR 31 May 2005, *Vetter v. France*, appl. no. 59842/00, and ECtHR 8 March 2011, *Goranova-Karaeneva v. Bulgaria*, appl. no. 12739/05, § 44.

communications.[126] The case law for the latter has already been examined in subsection 4.2.2 under D.

Required quality of the law
With regard to the quality of the law, the ECtHR specifically requires that the regulations that enable the interception of communications with covert listening devices are *particularly precise.* This is done to prevent an arbitrary governmental interference from taking place in the private lives of individuals.[127]

For example, in the case of *Khan v. The United Kingdom*, the ECtHR clarified that it requires that the law is *"sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures"*.[128] In this case, the investigative method was based on an internal guideline of the U.K. Home Office that authorised the investigative activities. The ECtHR made clear that it required statutory laws regulating the investigative method regarding the use of covert listening devices.[129] As such, the U.K. Home Office's internal guideline was not of sufficient quality.

In the case of *Goranova-Karaeneva v. Bulgaria*, the ECtHR further considered that the following four safeguards are appropriate for the use of covert listening devices: (1) a warrant describing the intended operation; (2) a restriction on the duration of the operation; (3) the possibility of a review to challenge the obtained evidence; and (4) the existence of procedures for preserving the integrity and confidentiality of the materials obtained through covert surveillance as well as for eventually destroying these materials.[130] With regard to the procedural safeguards for the regulation of the investigative method itself, (1) the warrant requirement and (2) a restriction on the duration of the investigative method are thus particularly important.

4.4.3 The right to privacy and hacking as an investigative method

This subsection analyses the gravity of the privacy interference when hacking is applied as an investigative method. It also considers whether the case law concerning the counterpart investigative methods examined above and their corresponding quality of the law requirements align with hacking as an investigative method.

---

126 See ECtHR 31 May 2005, *Vetter v. France*, appl. no. 59842/00, § 26 and ECtHR 8 March 2011, *Goranova-Karaeneva v. Bulgaria,* appl. no. 12739/05. Although case law does not explicitly states this, the required detailed regulations with specific procedural safeguards that are tested by the ECtHR indicates that the ECtHR views the privacy interference as serious.

127 See ECtHR 31 May 2005, *Vetter v. France*, appl. no. 59842/00, § 26.

128 ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 26.

129 ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 27. See also ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 38.

130 ECtHR 8 March 2011, *Goranova-Karaeneva v. Bulgaria,* appl. no. 12739/05, § 49-50.

Hacking as an investigative method is an umbrella term that encompasses different investigative methods that have in common that law enforcement officials *remotely access a computer system* (cf. Oerlemans 2011, p. 891). In this study, hacking as an investigative method comprises the following investigative methods: (A) network searches, (B) remote searches, and (C) the use of policeware on computers.[131] These methods are further examined below.

A Network searches

A network search is conducted when law enforcement officials are conducting a search of a place and find a computer that potentially contains evidence. In such a situation, law enforcement officials seize the computer and use it while it is still on, which enables them to gain access to interconnected devices and computers. As explained in subsection 2.4.3, a network search is also considered as a type of hacking as an investigative method in this study, because law enforcement officials can gain remote access to a computer system (of which the suspect is not necessarily aware) when a network search is performed. The investigative method is visualised in Figure 4.4. The reason Figure 4.4 is called a simplified model of a network search is that network searches can also take place in different places than a residence, such as inside an office and even inside a vehicle.

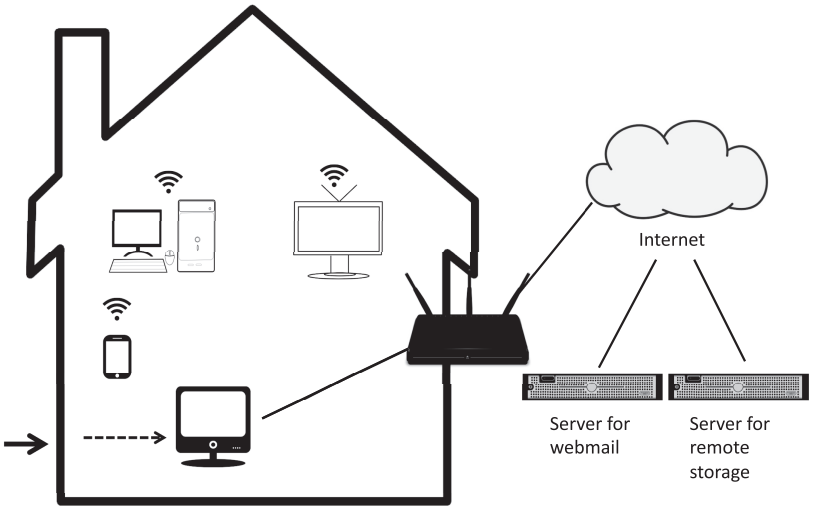

Figure 4.4: Simplified model of a network search.

Figure 4.4 illustrates how a network search is conducted at a certain place, such as a residence. Using a computer that is still on, law enforcement can use a network search as an investigative method to access the contents

131 See subsection 2.4.3.

stored on interconnected computers, such as an external hard disc that is shared with an internal network or an e-mail server that is used by a company but located elsewhere. Using a network search as an investigative method can also enable law enforcement officials to gain access to an individuals' webmail or online storage account when they seize a running computer (cf. Conings & Oerlemans 2013).[132] The prevalence of 'apps' on smartphones with accompanying login credentials and cloud services makes it possible for law enforcement officials to extract login credentials and use that information to subsequently collect evidence by performing a network search (insofar the smartphone is not encrypted).

Gravity of the privacy interference

Network searches and computer searches have important similarities as they are both conducted during the search of a place and involve analysing data stored on a computer. However, unlike a computer search, a network search also enables interconnected computers to be searched. Similar to regular computer searches, network searches also seriously interfere with the right to respect for home and correspondence as provided by art. 8(1) ECHR, with the difference that information can be obtained that is stored outside the location the initial search is conducted.

Alignment with the existing required quality of the law

The ECtHR requires detailed regulations for computer searches, (preferably) with the supervisory involvement of a judge who can authorise the search or conduct a retrospective judicial review. Since the gravity of the privacy interference is very similar for the investigative methods of computer and network searches, the quality of the law that is required aligns well for these investigative methods.

B Remote searches

During a remote search, law enforcement officials remotely access a computer that is located at a certain location. A remote search is different from a network search in that law enforcement officials do not 'physically' conduct computer searches at a certain place; it can instead be conducted 'virtually' from the convenience of a law enforcement official's desk. Remote searches are visualised in Figure 4.5.

132 Law enforcement officials can obtain login credentials from programs at the seized computer or from cookies to access certain web services. Login credentials can also be obtained through informants or voluntarily provided by a suspect.

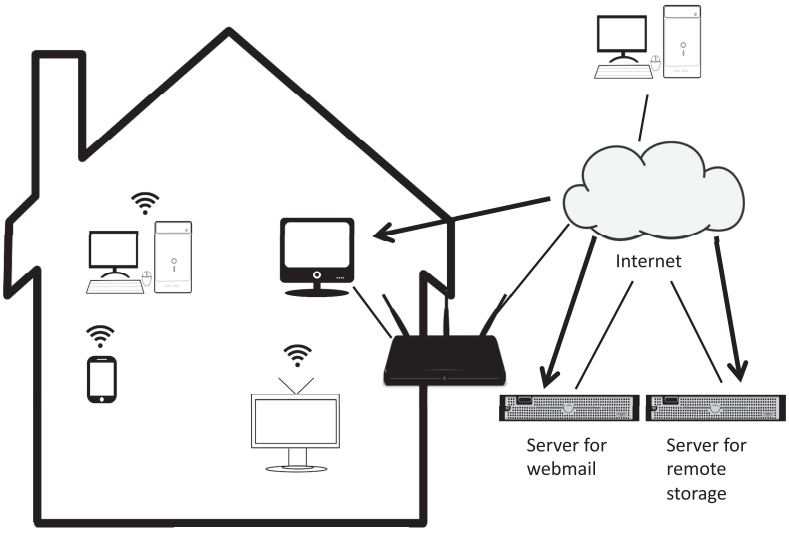

Figure 4.5: Simplified model of a remote search.

Figure 4.5 illustrates how a remote search distinguishes from computer searches and network searches. During a remote search, a computer is accessed remotely from a different computer through the Internet; not during a search at a place. An example of performing a remote search is when law enforcement officials log into a suspect's online account in order to search for information that is relevant to a criminal investigation.[133] The above model is simplified, because remote searches do not necessarily take place in computers located in the suspect's residence or in a suspect's webmail and online storage account.[134]

Gravity of the privacy interference

Remote searches clearly interfere with the involved individuals' right to respect for private life as meant in art. 8(1) ECHR (Oerlemans 2011, p. 898).[135] Based on the existing case law with regard to computer searches, it is expected that the investigative method will also interfere with the right to respect for home and correspondence.

The privacy interference that takes place during a remote search would be considered as serious by the ECtHR. During a remote search, law enforcement officials potentially gain access to sensitive information of individuals, such as photos, videos, and e-mails. I consider remote searches to be *more privacy intrusive* than computer searches, given that they are conducted

133 See also subsection 2.4.3 under B.

134 In addition, law enforcement officials will use anonymising services or techniques to obscure the origin of the hack.

135 See Groothuis & De Jong 2010, p. 280, Koning 2012, p. 49, and Koops et al. 2012b, p. 47.

covertly without presence of the suspect or other individuals. In contrast, the suspect is present when law enforcement officials physically search a place and seize a computer. In that situation, the suspect and perhaps even his lawyer can object to the seizure of certain data stored on computers. During a *remote* search, this is not an option.

Alignment with the existing required quality of the law
With regard to computer searches, in its case law the ECtHR prefers prior authorisation of an investigative judge to conduct the search. However, as argued above, remote searches should be considered more privacy intrusive than computer searches. For that reason, the required quality of the law for remote searches does not entirely align with the required quality of the law for regular computer searches.

The prior authorisation of an investigative judge should be regarded as a minimum requirement for remote searches. The ECtHR has repeatedly emphasised in other case law that investigative methods that are conducted covertly must be regulated in law in a 'particularly precise manner'.[136] Detailed procedures are required because applying the investigative methods in secret is accompanied by an increased risk of power being arbitrarily used, due to the diminished ability to control the investigative activity of a law enforcement authority.[137]

The required quality of the law for remote searches is thus likely to be (1) a detailed legal basis in statutory law and (2) prior authorisation from an investigative judge.

C The use of policeware
Before policeware can be utilised, law enforcement officials have to obtain remote access to a computer system that a suspect uses. The investigative method is visualised in Figure 4.6. The model of the use of policeware in Figure 4.6 is simplified, because law enforcement authorities will have to use their own ICT infrastructure to remain anonymous and exfiltrate the data from target computers in a secure manner. In addition, it is conceivable policeware is installed on different types of computers at any place (not only residences).

136 See ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 93, ECtHR 1 July 2008, *Liberty and Others v. the United Kingdom*, appl. no. 58243/00, § 62, and ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 61.

137 See, e.g., ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 67, ECtHR 24 April 1990, *Huvig v. France*, appl. no 11105/84, § 29, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 55.

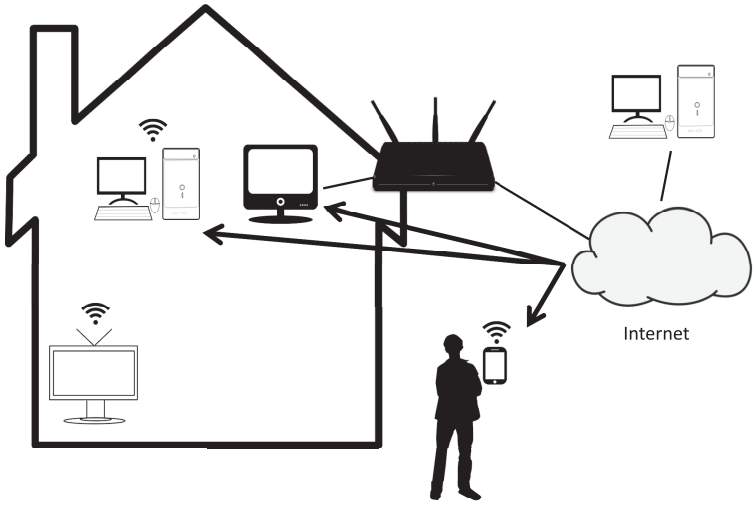

Figure 4.6: Simplified model for the use of policeware.

Figure 4.6 illustrates how law enforcement officials can remotely access any computer and install policeware regardless of their location. The use of policeware by law enforcement officials in criminal investigations interferes with the right to privacy in a different manner than network searches and remote searches. While these searches are focused on collecting certain information stored in a computer, policeware enables law enforcement officials *to monitor an individual's computer behaviours*. Policeware can enable law enforcement officials to take certain functions of a computer over for evidence-gathering purposes. For instance, they may be able to log keystrokes and turn a computer user's microphone on to intercept his communications. They can also take screen shots to see the activities of a computer user.[138]

Gravity of the privacy interference

The privacy interference that takes place when policeware is used is particularly serious. It can be placed at the far right of the scale of gravity for privacy interferences, given that the privacy interference is not restricted to looking at and copying private files (as is the case when a remote search is conducted). When policeware is used, law enforcement officials do not only gain covert remote access to a computer; they also *take over* the computer's functionalities. Essentially, law enforcement officials can 'spy' on a computer user's activities. This can take place quite literally by turning on a built-in camera without notifying the computer user. The use of policeware seriously interferes with the right with respect for private life, home, and correspondence as protected by art. 8 ECHR.

138 See also subsection 2.4.3 under B.

Alignment with the existing required quality of the law
The ECtHR already requires detailed regulations with strong procedural safeguards for the use of covert listening devices. Essentially, these safeguards consist of (1) a warrant requirement and (2) a restriction on the duration of the investigative method.[139] With regard to the required quality of the law, it is important to remember that in the last two decades the ECtHR has emphasised in its judgements with regard to the interception of (tele) communications that it is: *"essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated"*.[140] This statement can also serve as a warning for States that detailed regulations will be required for the use of policeware as an investigative method.

The use of policeware with its many functionalities interferes with the right to privacy more intensely than when covert listening devices are utilised. Nevertheless, the same quality of the law appears appropriate, because the highest level of detail of regulations and procedural safeguards are reached. In that respect, the quality of the law for policeware aligns with the required quality of the law for covert listening devices. Considering the intrusiveness of the investigative method, it appears that legislatures should also critically assess which application of the use of policeware is still regarded as 'necessary in a democratic society'.

4.4.4 Desired quality of the law

This subsection determines the *desirable* quality of the law based on the gravity of the privacy interference that takes place when hacking is applied as an investigative method.

In general, hacking as investigative method allows law enforcement officials to access computers located anywhere in the world and gather potentially large and diverse amounts of information. The three types of hacking used as investigative methods all seriously interfere with the right to privacy. Therefore, a detailed basis in statutory law with strong procedural safeguards is required to regulate the digital investigative method.

However, the three relevant types of hacking as an investigative method interfere with the right to privacy in different ways. The detailed regulations with procedural safeguards should therefore be tailored to the specific investigative method. The desirable quality of the law for the identified types of hacking as investigative methods is discussed below.

---

139 See the analysis in subsection 4.4.2.

140 ECtHR 24 April 1990, *Kruslin v. France*, appl. no. 11801/85, § 33. See also ECtHR 24 April 1990, *Huvig v. France*, appl. no. 11105/84, § 32, ECtHR 25 March 1998, *Kopp v. Switzerland*, appl. no 13/1997/797/1000, § 72, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 46, ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 93 and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 229.

A Network searches

The use of a network search as an investigative method interferes with individuals' right to privacy in a similar manner to a computer search, as it also occurs in a place search during which computers are seized. The gravity of the privacy interference is considered serious and can be placed at the right end of the scale of gravity for privacy interferences. In recent case law with regard to computer searches, the ECtHR has made clear that it prefers the involvement of an investigative judge as a procedural safeguard.

Considering the gravity of the privacy interference that takes place when a network search is performed, I view a *detailed legal basis in statutory law* for the investigative method as desirable. As a procedural safeguard for the regulation of the investigative method, prior *authorisation of an investigative judge* is desirable. As part of the authorisation (warrant) to conduct a network search, the scope of the network search should be restricted in the request for the warrant.

B Remote searches

Remote searches interfere with the right to privacy in a more intrusive manner than network searches do. The reason is that remote searches are conducted covertly, whereas computer searches are conducted in the presence of the suspect. The covert use of this intrusive investigative method is accompanied by a risk of an arbitrary use of governmental power.

The privacy interference that takes place when remote searches are conducted is therefore considered particularly serious and placed on the far (right) end on the scale of gravity for privacy interferences. For that reason, a *detailed legal basis in statutory law* is in my view appropriate for the regulation of this investigative method. In addition, prior *authorisation of an investigative judge* is the desirable procedural safeguard. As part of the authorisation (warrant) to conduct a remote search, the scope and duration of the remote search should be restricted in the warrant.

C The use of policeware

The use of policeware can be considered the most privacy intrusive investigative method that is examined in this study. Policeware allows law enforcement officials to monitor the computer behaviours of individuals by taking over the functionalities of a computer system, which then enables them to 'spy' on that computer user's activities.

In this study, the use of policeware is placed on the farthest right of the scale of gravity for privacy interferences. Considering the intrusiveness of this investigative method, it should have a *detailed legal basis in statutory law* to prevent arbitrary governmental interferences in the private lives of the individuals involved. Based on case law with regard to computer searches and the use of covert listening devices by law enforcement authorities, I consider (1) prior *authorisation of an investigative judge* to use of policeware and (2) a *restriction on the duration and functionalities* of the use of policeware as desirable procedural safeguards.

4.5 Chapter conclusion

The aim of this chapter was to identify the desirable quality of the law based on art. 8 ECHR for the regulation of the identified digital investigative methods (RQ 3). To answer RQ 3, the gravity of the privacy interference that takes place when the identified digital investigative methods are applied was examined and the accompanying quality of the law was formulated.

The first step in doing so was to analyse case law concerning similar investigative methods in order to identify the gravity of the privacy interference and accompanying quality of the law that the ECtHR requires in relation to those non-digital counterparts. This provided a basis for comparison with digital investigative methods.

As second step, the digital investigative methods were examined in detail to determine how they interfere with the right to privacy as defined in art. 8 ECHR. Whether the required quality of the law of the counterpart investigative methods aligns with the digital investigative methods was also analysed. The analysis showed that the privacy interferences caused by the digital investigative methods of (1) the gathering of publicly available online information, (2) the issuing of data production orders to online service providers, and (3) hacking as an investigative method, (which have not been examined in case law of the ECtHR) significantly differ from those caused by their non-digital counterparts that *have* been examined in case law by the ECtHR. Generally, the amount and diversity of information that can be processed when these digital investigative methods are applied significantly affects the gravity of the privacy interference. In my view, only the quality of the law requirements developed in case law for undercover investigative methods already aligns with the quality of the law requirements that are appropriate for the application of online undercover investigative methods.

As a third step, the results of the analysis conducted in the second step were used to determine the desirable quality of the law for the investigative methods.

Summary of the gravity of the privacy interferences and the desired quality of law
The result of the analysis that was conducted in sections 4.1 to 4.4 is presented in Table 4.1. This table provides an overview of the gravity of the privacy interferences that take place when each of the identified digital investigative methods is applied and the corresponding recommended desirable quality of the law for regulating the identified digital investigative methods.

Investigative method	Gravity of the privacy interference	Desirable level of detail for the regulations	Desirable procedural safeguards
Gathering publicly available online information:			
A. Manual gathering of information.	A. Minor interference.	A. General legal basis in law may suffice.	A. None (although data protection regulations apply).
B. Automated gathering of information.	B. More serious interference.	B. Detailed legal basis in law in statutory law or public guidelines.	B. None (although data protection regulations apply).
C. Observation of online behaviours of individuals.	C. Minor interference.	C. Detailed legal basis in statutory law or public guidelines.	C. None (although data protection regulations apply).
Issuing data production orders:			
A. Subscriber data.	A. Minor interference.	A. Detailed legal basis in statutory law.	A. No specific procedural safeguards required.
B. Traffic data.	B. Serious interference.	B. Detailed legal basis in statutory law.	B. Authorisation from an investigative judge.
C. Other data.	C. Serious interference.	C. Detailed legal basis in statutory law.	C. Authorisation from an investigative judge.
D. Content data.	D. Particularly serious interference.	D. Detailed legal basis in statutory law.	D. Authorisation from an investigative judge.
Applying undercover investigative methods:			
A. Pseudo-purchases.	A. Minor interference.	A. Detailed legal basis in statutory law.	A. Supervision by a public prosecutor.
B. Online undercover interactions with individuals.	B. Serious interference.	B. Detailed legal basis in statutory law.	B. Supervision by an investigative judge.
C. Online infiltration operations.	C. Serious interference and increased risks regarding the integrity of investigations.	C. Detailed legal basis in statutory law.	C. Supervision by an investigative judge.
Performing hacking as an investigative method:			
A. Network searches.	A. Serious interference.	A. Detailed regulations in statutory law.	A. Authorisation from an investigative judge.
B. Remote searches.	B. Particularly serious interference.	B. Detailed regulations in statutory law.	B. Authorisation from an investigative judge.
C. The use of policeware.	C. Particularly serious interference.	C. Detailed regulations in statutory law.	C. Authorisation from an investigative judge and a restriction of the duration and functionalities of the use of policeware.

Table 4.1: Overview of the gravity of the privacy interferences caused by the identified digital investigative methods and the corresponding recommended desirable quality of the law.

5 Gathering publicly available online information

This chapter aims to answer the fourth research question with regard to the gathering of publicly available online information (RQ 4a): *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate the gathering of publicly available online information?* Within this study, the investigative method of gathering publicly available online information is subdivided into (1) the manual gathering of publicly available online information, (2) the automated gathering of such information, and (3) the observation of online behaviours of individuals. To answer this research question, the investigative method is placed within the Dutch legal framework and further analysed to determine whether Dutch law meets the normative requirements. In chapter 3, these normative requirements were identified as follows: (1) accessibility, (2) foreseeability, and (3) the quality of the law.

In chapter 4, it was determined for each method what degree of privacy interference is involved in its application. By positioning each method on the interference 'scale', it was further determined which type of regulation is required in each case, ranging from (a) a general legal basis for light interferences, (b) detailed regulations in statutory law or guidelines for more serious interferences that restrict the investigative method (with regard to specific crimes, in duration, et cetera) and (c) detailed regulations in statutory law that restrict the investigative method with the procedural safeguard of authorisation of an investigative judge for very serious interferences. The more serious the interference, the stricter are the requirements for the (1) accessibility, (2) foreseeability, and (3) the quality of the law. In case law, the ECtHR does not always strictly separate the three normative requirements and consider them all as part of the quality of the law.[1] However, in this study, these normative requirements are examined separately. The requirement of the quality of the law focuses in this research on the level of detail of the regulations and procedural safeguards that are present in the regulations for the investigative method.

1 See, e.g., ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 44: *"The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law; secondly, it refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and that it is compatible with the rule of law"*

For the method of gathering publicly available online information, the analysis in subsection 4.1.3 showed that data protection regulations should apply as a baseline for this investigative method. The specific requirements that are further desirable for the regulation of the three distinguished categories of gathering publicly available online information differs per method.

Case law indicates that the ECtHR takes into consideration the fact that the type of information at issue here is publicly available to everyone, including law enforcement authorities. At the same time, the more information these authorities gather and process, the greater becomes the privacy interference that takes place. Legislators should create an adequately detailed legal basis for each variant of the investigative method in which the right to privacy is properly balanced with the particular privacy interference involved in each case. It must be noted here that ECHR rights only specify the minimum level of protection required for the individuals involved. Contracting States to the convention can incorporate further requirements in the legal frameworks that regulate the different types of information gathering used as investigative methods. In this regard, before proceeding, it is important to highlight important aspects of the Dutch legal framework that pertain to regulating investigative methods. This overview is also relevant for the analysis of the other three digital investigative methods, which is presented in chapters 6 to 8.

Features of the Dutch legal framework for investigative methods

As explained in section 1.1, the Netherlands has a civil law system with a strong commitment to the principle of legality. This is particularly the case in criminal and criminal procedural law. In criminal procedural law, as laid down in art. 1 DCCP, the legality principle prescribes that *"criminal procedure is only carried out in the manner provided by law"*.[2] Here 'law' refers to statutory law that is established by acts of the Dutch House of Representatives and reviewed by the Dutch Senate.

In the context of regulating investigative methods, the implication is that – in principle – investigative methods are regulated by statutory law. However, not all investigative methods are covered in detail in statutory law. Over time, the general rule has developed that investigative methods that (1) do not – or only in a minor way – interfere with the fundamental rights and freedoms of individuals and (2) do not endanger the integrity of criminal investigations do not require detailed regulations in criminal

2 See art. 1 DCCP.

procedural law.[3] Investigative methods that interfere with fundamental rights and freedoms of individuals in more than a minor manner or endanger the integrity of criminal investigations do require detailed regulation in law. In Dutch criminal procedural law, the possibility also exists to regulate administrative or technical aspects of investigative methods outside of criminal procedural law in lower regulations than statutory law.[4]

Similar to the *scale of gravity for privacy interferences* that was deduced from art. 8 ECHR, under Dutch law, the more that investigative methods interfere with the rights and freedoms of the involved individuals or threaten the integrity of criminal investigations, the more detailed the regulations for investigative methods must be, with more accompanying safeguards.[5] An important structural safeguard in this regard lies in the fact that, the law will determine who has the power to apply and authorise the application of investigative powers. Depending on the gravity of the power, that authority will be higher, ranging from (1) a law enforcement official[6], (2) a public prosecutor, or (3) an investigative judge. Furthermore, these powers are generally

3 The investigative method is then based upon art. 3 of the Dutch Police Act and art. 141 in conjunction with 142 DCCP. See also, e.g., Fokkens & Kirkels-Vrijman 2009 in: Borgers, Duker & Stevens (ed.) 2009 and Borgers 2015. This standard was first set in the landmark case of *Zwolsman* in 1995, in which the Dutch Supreme Court decided that searching trash bags of citizens was not a privacy-infringing investigative method to the extent that it required detailed regulations in the Dutch Criminal Procedural Code (HR 19 December 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996, 249 m. nt. Schalken). The standard was later affirmed with regard to other investigative methods by the Dutch legislature in the explanatory memorandum to the Special Investigative Powers Act (*Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3, p. 110 and 115) and the Dutch Supreme Court (see, e.g., HR 20 January 2009, ECLI:NL:HR:2009:BF5603, *NJ* 2009, 225, m.nt. Borgers, HR 13 November 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013, 413, m.nt. Borgers and HR 7 July 2014, ECLI:NL:PHR:2014:623). The literature reflects conflicting viewpoints concerning whether investigative methods that do not interfere with the rights and freedoms of individuals involved require a legal basis (cf. Knigge & Kwakman 2001, p. 193-205 and p. 310-325 in: Groenhuijsen & Knigge 2001).

4 See also the letter regarding the contours of the 'Modernising Criminal Procedural Law' project of 30 September 2015, p. 10-11. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (last visited on 23 March 2016). Borgers (2015) suggested that lower regulations can also be created for investigative methods that only interfere with the rights and freedoms of individuals in a minor manner and do not threaten the integrity of criminal investigations (cf. Borgers 2015).

5 In literature, there are also other reasons identified why investigative methods should be regulated in specific provisions in Dutch criminal procedural law, such as (1) to secure the reliability of the process of evidence-gathering, (2) to secure the right to fair trial in art. 6 ECHR, (3) to increase control checks and transparency of the evidence gathering-activity, (4) to fight corruption that may be take place in evidence-gathering activities, and (5) to protect the interests of others (besides the suspect) that may be involved in the application of investigative methods (see Groenhuijsen & Knigge 2002, p. 323-326).

6 In Dutch law, higher ranking law enforcement officials exist (called deputy prosecutors), which may authorise certain investigative activities. These are not further examined in this study.

restricted by limiting their application to criminal investigations with regard to certain crimes based on a crime's severity, as this is determined by the maximum sentence that can be imposed for that crime.

In essence, the regulations for investigative methods in Dutch law are similar to the scale of gravity for privacy interferences and the quality of the law that can be derived from art. 8 ECHR (see subsection 3.3.4). Again, depending on the gravity of the power, its regulation can be restricted by way of delineation of scope of application (in terms of manner and situations in which it can be applied), duration (including possibilities for extension), through stricter reporting requirements, and stricter proportionality and subsidiarity requirements.[7] The detail of these regulations both influences foreseeability (by indicating the manner the investigative method is applied) and the quality of the law (the level of detail and authorisation levels to apply the investigative methods). Throughout the chapters 5-8, the focus on the regulations for investigative methods is on the main mechanisms by restricting investigative methods based on authorisation requirements and limiting the application to the investigation of certain crimes. The higher level of detail for regulations is achieved by these restrictions. The heightened legality principle in Dutch criminal procedural law means that investigative methods will usually have a legal basis in Dutch law. However, the accessibility of digital investigative methods can be problematic when it is not recognised a digital method is distinct to its counterpart investigative method and requires its own regulation due to its intrusiveness. There can thus be an overlap in the issues of accessibility and foreseeability. From this chapter to chapter 8, it is examined whether the Dutch law currently correctly places the privacy interference that accompanies each investigative method on the scale of gravity and adequately regulates these investigative methods.

Structure of the chapter

This chapter is structured on the basis of the three normative requirements, each of which is investigated in a separate section. Each section discusses all three categories of the gathering of publicly available information in a subsection. A fixed research scheme is used to assess the accessibility and foreseeability of the Dutch legal framework with regard to the investigative methods. This research scheme consists of examining (A) statutory law, (B) legislative history, (C) case law, and (D) public guidelines. Thereafter, it is analysed whether Dutch law meets the normative requirements for regulations, which are extracted from art. 8 ECHR in chapter 4. Based on

7 Customary principles of proper criminal procedure, including those of proportionality and subsidiarity, as well as the prohibition of abuse of power also always apply to the exercise of criminal procedural powers, even though they are not stipulated explicitly by law.

the results of the analyses, recommendations are provided to improve the Dutch legal framework.[8]

Section 5.1 thus tests the *accessibility* of the Dutch legal framework's basis for applying the investigative method in the Netherlands, while section 5.2 examines to which extent the method is regulated in a *foreseeable* manner. Section 5.3 analyses whether the Dutch legal framework meets the desired *quality of the law* in the sense that it provides adequate level of detail for the regulations with adequate procedural safeguards. Based on the results of the analyses conducted in these three sections, section 5.4 provides concrete proposals as to how Dutch criminal procedural law can be improved to adequately regulate the gathering of publicly available online information. Section 5.5 concludes the chapter by presenting a summary of the findings.

5.1 Accessibility

An accessible basis in law means that the individual involved has an adequate indication of which regulations apply to the use of investigative methods in a particular case.[9] This section examines the accessibility of the regulations with regard to the gathering of publicly available online information.

As explained above, due to the heightened legality principle in Dutch criminal procedural law, it is expected that the legal basis for investigative methods will be accessible. It is rare that Dutch law enforcement authorities use secret internal guidelines and that such guidelines provide the legal basis for the application of investigative methods. However, it is possible that a digital investigative method is so novel that it has not yet been assigned a legal basis or that the Dutch legislature has failed to both distinguish it and create the corresponding detailed regulations that it requires. In that sense, the law may not be accessible, because there is no distinct clear legal basis for the digital variant.

The accessibility of all three categories of gathering publicly available online information is examined separately in subsections 5.1.1 to 5.1.3. Subsection 5.1.4 presents conclusions regarding the accessibility of the investigative method in Dutch law.

8 The recommendations are provided in section 5.4, as opposed to in each section that analyses the adequacy of the Dutch legal framework in terms of the identified normative requirements. This is done to present the relationships between these recommendations in a clearer manner.

9 See subsection 3.2.2 under A.

5.1.1 Manual gathering of publicly available online information

The manual gathering of publicly available information has been compared to the gathering of information from open sources, such as newspapers and telephone directories. In an online context, publicly available information can be manually gathered by utilising search engines and by gathering information from online forums and social media services. The accessibility of this investigative method in Dutch law is examined below using the research scheme that is mentioned in the introduction to this chapter.

A Statutory law

The manual gathering of publicly available online information is not regulated in detail in the DCCP. The investigative method can be based on the general task description for law enforcement officials to investigate crimes that is contained in art. 3 of the Dutch Police Act, insofar as the investigative method (1) does not interfere – or interferes in only a minor way – with the fundamental rights and freedoms of individuals and (2) does not endanger the integrity of criminal investigations. Art. 3 of the Dutch Police Act reads as follows:

"The police have the task, subordinate to the competent authority and in compliance with the applicable rules, to ensure the effective enforcement of the law and provide assistance to those in need".[10]

This provision itself does not explicitly state that law enforcement officials can derive from it the authority to investigate crimes and therewith apply investigative acts that interfere with the right to privacy. It only describes the broad task description of law enforcement officials. The task of criminal law enforcement, including the investigation of crimes, falls under the task of the effective enforcement of the law. The competent authority in that context is the public prosecutor. Given the general nature and broadness of this provision, it can be concluded that statutory law itself does not provide a distinct explicit legal basis for the manual gathering of publicly available online information.

B Legislative history

In 1999, the Minister of Justice stated in its explanatory memorandum to the Computer Crime Act II that: *"law enforcement officials can look around in the digital world and take notice of publicly available information just like anyone else*".[11] It added that *"an explicit basis in law is not required for this activity, insofar the activities are part of the tasks of law enforcement authorities"*.[12] No mention is

10 All translations of the statutory provisions are made by the author.

11 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35.

12 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35.

made about the investigative method in the explanatory memorandum to the Special Investigative Powers Act.

The explanatory memorandum then specified that: "*the power to look around on a publicly accessible network does not imply the power to systematically download information about individuals from the Internet and store that information in police systems*".[13] Thereafter it warned that the gathering of information from the Internet is regulated by *data protection regulations* that restrict this type of evidence gathering to the degree that it is necessary to properly execute the police task.[14]

Dutch legislative history thus indicates that this investigative method can be based on art. 3 of the Dutch Police Act, whilst it is further restricted by data protection regulations. In the literature, this view is supported by Van der Bel, van Hoorn, and Pieters (2013, p. 325). At the same time, the explanatory memorandum to the Computer Crime Act II states that a distinct legal basis is required for the application of the investigative method, i.e., a special investigative power in the DCCP, *"as soon as the investigation can be characterised as 'systematic'"*.[15] However, it does not state which special investigative power should apply in such a case. Koops (2012, p. 34) argues that the special investigative power for systematic observation applies when information is systematically gathered from the Internet. The special investigative power for systematic observation is formulated in art. 126g(1)DCCP Dutch as follows:

"In case of reasonable suspicion of a crime, a public prosecutor can order a law enforcement official to systematically follow a person or systematically observe the behaviours of a person, insofar this is in the interest of the investigation"[16].

In contrast to what I argued in 2012 (Oerlemans & Koops 2012, p. 45), I no longer think that this special investigative power provides the proper legal basis for the investigative method at hand. The investigative method of observation concerns gathering evidence in a criminal investigation by following a person or systematically observing his behaviours. As such, the method starts at a specific moment in time. *From that moment on*, information is gathered using the investigative method of observation. In contrast, the manual gathering of publicly available online information concerns the gathering of information that has been generated *in the past*. For that reason,

13 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

14 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

15 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

16 Emphasis added. The relevant requirements to apply the investigative method are examined in section 5.2. As explained in subsection 1.3.2, only the provision for ´classical investigations´ (in Title IV and IVA of the DCCP) are examined.

observation in the sense of art. 126g DCCP does not take place when this method is applied.[17]

To conclude, legislative history indicates on the one hand that the investigative method can be based on art. 3 of the Dutch Police Act and that the investigative method is restricted by data protection regulations. On the other hand, legislative history warns that the investigative method cannot be applied systematically on this basis, yet does not indicate which special investigative power can provide the appropriate legal basis for the investigative method.

C Case law

There is only *one* Dutch case available that explicitly deals with the legitimacy of the manual gathering of publicly available online information by law enforcement officials.[18] This case concerns a financial fraud investigation in 2004 in which a law enforcement official used 'Google Earth' to zoom in on the suspect's garden to ascertain whether the suspect had fraudulently acquired specific chairs and had them shipped to his home address instead of a company address. The investigating officer ascertained with the use of Google Earth that the two 'Bubble Club' chairs ordered were indeed located in the suspect's garden, which provided important evidence that the suspect had committed fraud.

The suspect's lawyer objected to the online evidence-gathering activity. He argued that the investigative method was unlawful, stating that the investigative act should have been based on a special investigative power regulated in the DCCP (although he did not specify which one), since the investigative method interferes with the right to privacy in more than minor manner.

The Court of The Hague disagreed with the suspect's lawyer, finding that the evidence-gathering activity only led to a minor interference with the individual's right to privacy. The activity could therefore be based on art. 3 of the Dutch Police Act.[19] The court also recalled the relevant legislative history and stated that online information cannot be 'systematically gathered and downloaded in police systems' upon the general legal basis of art. 3 of the Dutch Police Act. In this case, no systematic gathering of information had taken place in this case according to the court.

Thus, the only case that is available indicates that law enforcement officials can utilise Google Earth for evidence-gathering purposes based on art. 3 of the Dutch Police Act.

17 See also CTIVD 2014, p. 9 and p. 42.

18 Rb. Den Haag, 23 December 2011, ECLI:NL:RBSGR:2011:BU9409.

19 However, the judges did warn in their verdict that law enforcement officials are *"not allowed to systematically download information from the Internet and store it in police files"* on the legal basis of the description of the statutory duty of law enforcement officials to investigate crime. With this statement, the judges clearly refer to the legislative history cited above, in which this threshold is also mentioned.

D Public guidelines

The Guideline for the Special Investigative Powers of the Public Prosecution Service from 2014 only states that law enforcement officials are not required to issue data production orders to obtain information that is publicly accessible.[20] Data production orders are regulated as special investigative powers in Dutch criminal procedural law. These regulations are extensively analysed in chapter 6.

Within the guideline, the 'public part of the Internet' is provided as an example of information that is publicly accessible.[21] The guideline does not specify which other special investigative powers may apply in the context of gathering publicly available information. Here it is noteworthy that the guideline also does not differentiate between the (1) manual gathering of publicly available online information, (2) automated gathering of publicly available online information, and (3) the observation of online behaviours of an individual. The guideline also does not refer to any special investigative power that may provide a detailed legal basis for the systematic gathering of publicly available online information. It can be taken as a point of departure therefore that the Guideline for Special Investigative Powers implicitly holds that the gathering of publicly available online information can be based on art. 3 of the Dutch Police Act.

5.1.2 Automated gathering of publicly available online information

The automated gathering of publicly available online information differs from the manual gathering of such information in the sense that it involves using automated data collection systems. The accessibly of the regulations for the investigative method are examined below using the announced research scheme.

A Statutory law

The automated gathering of publicly available online information is not regulated in specific provisions of the DCCP. Again, the general legal basis in art. 3 of the Dutch Police Act may apply. As said, this is a general and broad provision and does not refer to any particular method.

Statutory law therefore does not provide a distinct explicit legal basis for the automated gathering of publicly available information.

B Legislative history

The explanatory memoranda of the Special Investigative Powers Act and the Computer Crime Act II both do not refer to this investigative method. The latter mentions that *law enforcement officials* can 'look around on the

20 *Stcrt.* 2014, no. 24442.

21 See section 2.10 in the Guideline for Special Investigative Powers.

Internet'.[22] However, this is different from the automated gathering of publicly available online information, which involves *software* collecting information automatically. However, in 2013, the Dutch government mentioned that the use of the 'iColumbo' automated online data collection system meets the Dutch Police Files Act's requirements for storing personal information about individuals in police systems.[23] This statement implies that the investigative method can be based on art. 3 of the Dutch Police Act and that the investigative method is only restricted by data protection regulations. As explained in subsection 2.2.2, the Dutch iColumbo system reportedly aims to provide *"an 'intelligent, automated, "near" real-time Internet monitoring service' for governmental investigators"*.[24]

Legislative history thus indicates that the investigative method can be based on art. 3 of the Dutch Police Act and that data protection regulations apply to the automated gathering of publicly available online information.

C Case law

No Dutch case law is available with regard to the automated gathering of publicly available online information as an investigative method.

D Public guidelines

The Guideline for Special Investigative Powers also fails to mention the automated gathering of publicly available online information as an investigative method. As explained under D in subsection 5.1.1, this guideline only specifies that no data production orders are required to obtain information from publicly accessible parts of the Internet.[25] The guideline does not differentiate between various types of gathering of publicly available online information.

The guideline therefore provides no indication of the legal basis for applying this investigative method.

5.1.3 Observation of online behaviours of individuals

Observing the online behaviours of individuals is an investigative method that takes place on publicly accessible places on the Internet, such as online forums, chat services and social media, insofar as anyone can observe that information. The observation of online behaviours of individuals starts at a

22 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35 and subsection 5.1.1 under B.

23 See the memorandum 'Freedom and safety in the digital society. An agenda for the future' of 14 December 2013, 26 643, no. 298, p. 12.

24 See 'Deelprojectvoorstel, Ontwikkeling Real Time Analyse Framework voor het iRN Open Internet Monitor Network', 'iColumbo'. Available at http://www.nctv.nl/Images/deel-projectvoorstel-ontwikkeling-icolumbo-alternatief_tcm126-444133.pdf (last visited 23 December 2015).

25 See section 2.10 of the Guideline for Special Investigative Powers.

specific point in time and therefore does not entail the gathering of information from individuals that has been published in the past. As such, it differs from the investigative method of manual and automated gathering publicly available online information.[26] The accessibility of the legal basis for this investigative method is examined below using the announced research scheme.

A Statutory law

For the observation of online behaviours, the legal basis for the special investigative power for systematic observation in art. 126g DCCP may be appropriate. As explained in section 5.1.1, this provision describes this evidence gathering-activity as *following a person* or *observing the behaviours of an individual*. This text does not restrict the investigative method to application in the physical world.[27]

However, the special investigative power only applies when the observation is *systematic* in nature. The *non-systematic* observation of behaviours of individuals can be based on art. 3 of the Dutch Police Act.

B Legislative history

In 1999, in the explanatory memorandum to the Computer Crime Act II, it was noted that the point of departure is that special investigative powers, such as systematic observation, can also be applied in the digital world.[28] It also stated that special investigative powers that are applied online must fulfil the same conditions as those that are applied in the physical world.[29] The explanatory memorandum of the Special Investigative Powers explicitly states that non-systematic observation can be based on art. 3 of the Dutch Police Act (then art. 2).[30] As a consequence, systematic online observation requires the special investigative power of systematic observation and the non-systematic online observation can be based on art. 3 of the Dutch Police Act.

Legislative history thus clearly indicates that the current regulations for observation in Dutch criminal procedural law also apply in an online context.

---

26 For a similar distinction, see p. 86-87 of the explanatory memorandum of the new bill for the Security and Intelligence Services Act and CTIVD 2014, p. 9 and p. 42.

27 The explanatory memorandum to the Special Investigative Powers Act explicitly states that the special investigative powers are formulated in a 'technological neutral manner' (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 55).

28 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

29 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

30 see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 110.

C Case law

No case law that specifically addresses the observation of the online behaviours of individuals as an investigative method is available. A large amount of case law is available concerning observation in the physical world.[31] However, this case law does not indicate which legal basis applies to *online* observations, i.e., art. 3 of the Dutch Police Act or the special investigative power for systematic observation.

Case law therefore does not indicate the legal basis for the examined investigative method.

D Public guidelines

The Guideline for Special Investigative Powers specifies how the special investigative power for systematic observation can be distinguished from other special investigative powers.[32] This distinction is as follows. The investigative method of observation involves law enforcement officials *passively observing the behaviours* of an individual to gather evidence in a criminal investigation,[33] while undercover investigative methods entail law enforcement officials that *interact with an individual in an undercover capacity* to gather evidence.[34]

The guideline refers to legislative history to determine when observation becomes systematic (see subsection 5.2.3) and specifies the recommended procedure to make use of a special observation team to apply the special investigative power.

In contrast to legislative history, the guideline does not explicitly state that the investigative method can also be applied in an online context.

5.1.4 Section conclusion

The analysis above has shown that Dutch law does not distinguish between the various types of gathering of publicly available information as they have

31 When using the Dutch equivalents of the search terms 'systematic observation' and 'procedural defects' on the website www.rechtpraak.nl, 195 cases are available for analysis (on 23 July 2016). This website offers a large database of case law that is uploaded by Dutch courts. In most of these cases, the legal basis to use observation as an investigative method is contested by the suspect. After a thorough analysis, *none* of these cases concerns the online observation of individuals' behaviours.

32 See section 2.6 of the Guideline for Special Investigative Powers.

33 See also Oerlemans & Koops 2012, p. 43.

34 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 35. See also Buruma 2001, p. 84-85 and Corstens & Borgers 2014, p. 506. The legislature emphasised in its explanatory memorandum to the Special Investigative Powers Act that the investigative method of 'systematic information gathering' implies 'more than just listening or observing'. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 38 indicating the investigative method of 'systematic information gathering' must only be used when the undercover investigator *engages in a conversation* with a suspect.

been described as distinct categories in this study. In the explanatory memorandum to the Computer Crime Act II, reference is only made to the gathering of publicly available online information and the observation of online behaviours. In this study, a distinction is made between (1) the manual gathering of publicly available online information, (2) the automated gathering of publicly available online information, and (3) the observation of online behaviours of individuals.

With regard to the manual gathering of publicly available online information, the explanatory memorandum to the Computer Crime Act II indicates that the investigative method can be based on art. 3 of the Dutch Police Act. According to legislative history, a special investigative power must be applied for the 'systematic' gathering of publicly available online information. Given this, Dutch law can be considered *accessible* for this investigative method, in the sense that there is an indication of which legal basis applies. However, it remains unclear from the examined legal sources which special investigative power is applicable when the manual gathering becomes systematic.

Dutch legislative history indicates that the Dutch automated data collection system of 'iColumbo' can be based on art. 3 of the Dutch Police Act and that the use of the system is restricted by data protection regulations. Therefore, again there is an *accessible* legal basis for the automated gathering of publicly available online information.

With regard to the investigative method of observing online behaviours of individuals, the explanatory memorandum to the Dutch Computer Crime Act II and statutory law also provide an indication of what the legal basis is. The former is most concrete and makes it clear that the investigative method can be based either on (1) the description of the statutory duty of law enforcement officials to investigate crimes that is provided in art. 3 of the Dutch Police Act or (2) the special investigative power for systematic observation that is contained in art. 126g of the DCCP. The legal basis for applying this investigative method is therefore considered as *accessible*.

5.2 Foreseeability

The fact that an accessible legal basis exists however is only one of the requirements that flow forth from art. 8 ECHR for the regulation of investigative methods. That legal basis must also be foreseeable. A foreseeable legal framework is one that prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which an investigative method is exercised.[35] As such, given that a relationship exists between the gravity of a privacy interference and the degree of detail in which the method at issue must be regulated, the foreseeability

35 See subsection 3.2.2 under B.

requirement is particularly important. It is in the context of this requirement that the balancing and fine-tuning of the interference and the detail of the regulation must be achieved.

The foreseeability of the Dutch legal framework for all three categories of gathering publicly available online information is examined in subsections 5.2.1 to 5.2.3. Subsection 5.2.4 then draws conclusions regarding the investigative methods' foreseeability in Dutch law.

5.2.1 Manual gathering of publicly available online information

This subsection examines whether the manual gathering of publicly available online information is regulated in a foreseeable manner by exploring the same legal sources used above.

A Statutory law

The analysis in subsection 5.1.1 has shown that the manual gathering of publicly available online information can be based on the general description of the duty of law enforcement officials to investigate crime in art. 3 of the Dutch Police Act, insofar as the investigative method is not applied in a systematic manner. When information is gathered in a systematic manner, a special investigative power should apply. However, the examined sources in law do not indicate which special investigative power should apply. In addition, the explanatory memorandum to the Dutch Computer Crime Act II does not elaborate on what determines the difference between systematic and non-systematic application of this investigative method. The scope of this investigative method thus remains unclear.

The general legal basis provided in art. 3 of the Dutch Police Act does not restrict this investigative method in a concrete manner. Law enforcement officials are authorised to apply investigative methods based on this legal basis in criminal investigations with regard to any crime. However, the explanatory memorandum to the Computer Crime Act II indicates that data protection regulations do restrict the investigative methods. Indeed, several authors emphasise that data protection regulations apply to this investigative method, even though it is not restricted by detailed regulations in criminal procedural law (cf. Koops 2012a, p. 32, Van der Bel, van Hoorn & Pieters 2013, p. 325, and Lodder et al. 2014, p. 73).[36]

36 Lodder et al. refer to opinion 03/2013 of the 'Article 29' Data Protection Authority Working Group of 2 April 2013, stating that: *"In this context, it is important to note that any information relating to an identified of identifiable natural person, be it publicly available or not, constitutes personal data. Moreover, the mere fact that such data has been made publicly available does not lead to an exemption from data protection law. The reuse of personal data made publicly available by the public sector, thus remains subject in principle to the relevant data protection law."* (at 10). See Koops et al. (2012, p. 41-43) with regard to data protection law and the collection of publicly available information from the Internet.

B Legislative history

The explanatory memorandum to the Computer Crime Act II specifies the scope of the investigative method. To a certain extent, it also specifies the manner it is executed.

Essentially, legislative history indicates that law enforcement officials can (1) 'look around on the Internet', (2) download relevant information from a variety of sources, and subsequently (3) store that information in police databases as part of their statutory duty to investigate crime.[37] The aforementioned explanatory memorandum also states that law enforcement officials can mask their IP addresses and use pseudonyms in order to remain undetected in their evidence-gathering activities.[38]

However, as mentioned above, the legislative history does not clarify what determines when information is gathered in a 'systematic manner' and when the application of a special investigative power is appropriate.

C Case law

The case law analysis in subsection 5.1.1 showed that only one case specifically deals with the manual gathering of publicly available online information by law enforcement officials. This case showed that law enforcement officials can make use of Google Earth based on art. 3 of the Dutch Police Act, thus without being bound to the detailed frameworks that apply for specific special investigative powers. This case thus does not provide much information about the scope of the investigative method. For instance, it remains unclear whether it makes a difference (1) if information is gathered from social media services instead of Google Earth or (2) if law enforcement officials may utilise commercial 'intelligence' providers that collect publicly available online information based on art. 3 of the Dutch Police Act.

D Public guidelines

The Guideline for Special Investigative Powers does not provide an indication concerning the scope of the investigative method or the manner in which law enforcement officials are to apply it.

5.2.2 Automated gathering of publicly available online information

This subsection examines the foreseeability of the legal basis for the automated gathering of publicly available online information. In subsection 5.1.2, it became clear that only one letter to Dutch parliamentary members indicated that the investigative method can be applied on the basis of art. 3 of the Dutch Police Act and that data protection regulations apply to this investigative method. However, there are no sources in law that indicate

37 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35-36.

38 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35.

how Dutch law enforcement officials should interpret these regulations in concrete terms (cf. Lodder & Schuilenburg 2016, p. 152).

The research results show that there is a clear misalignment between current practice and the limited description of the gathering of publicly available online information in legislative history. The explanatory memorandum to the Computer Crime Act II only specifies that law enforcement officials may (1) 'look around on the Internet', (2) download relevant information from a variety of sources, and (3) store that information in police databases as part of their statutory duty to investigate crime.[39] In practice, commercial and public automatic data collection systems download publicly available online information for law enforcement purposes every day.[40] That information is subsequently analysed and presented to law enforcement officials in the most efficient manner possible.

Automated data collection activities thus significantly extend beyond 'looking around on the Internet' for evidence-gathering purposes. As argued in section 4.1, this investigative method seriously interferes with the right to privacy and requires detailed regulations in either statutory law or public guidelines. The lack thereof can be explained by the fact the examined legislative history dates back to 1999. However, given the technological developments since then and the reality that this method is used, detailed regulation is currently necessary.

5.2.3 Observation of online behaviours of individuals

In this subsection, the foreseeability of the legal basis for observing the online behaviours of individuals is further examined by exploring the same legal sources used above.

A Statutory law

The analysis in subsection 5.1.3 has shown that the investigative method of the observation of online behaviours of individuals can be applied either on the basis of art. 3 of the Dutch Police Act or the special investigative power for systematic observation in art. 126g DCCP. If the investigative method is not applied systematically, a law enforcement official can observe the online behaviours of individuals based on art. 3 of the Dutch Police Act. This means that the investigative method can then be applied in as part of criminal investigations related to all crimes. In contrast, when it is applied systematically, the special investigative power for systematic observation must be used.

The special investigative power for systematic observation regulates this investigative method in detail. It specifies that it can be applied in criminal investigations involving all types of crimes, insofar as the investiga-

39 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35-36.

40 See subsection 2.2.2.

tive method is in the interest of the investigation. A public prosecutor must authorise the application of the special investigative power. Art. 126g DCCP also dictates that the special investigative power can only be applied for a maximum period of three months, which can be extended by another three months.[41]

Statutory law thus clearly describes the manner in which the investigative method should be applied, on two different legal bases. However, from statutory law alone it is not clear when (online) observation becomes 'systematic' in nature.

B Legislative history

The explanatory memorandum to the Special Investigative Powers Act specifies the scope of this investigative method by indicating when the method becomes systematic and the special investigative power for systematic observation is thus applicable.[42]

In 1996, the Dutch legislature formulated the following five factors for determining whether observation is systematic: (1) duration, (2) place, (3) intensity, (4) frequency, and (5) whether a technical device is used to observe an individual's behaviours.[43] These five factors – 'particularly in their combination' – indicate "*whether more or less complete insights are obtained about certain aspects of an individual's private life*" and thus if the investigative method is being applied systematically.[44]

Application in an online context

The aforementioned five factors are designed for the physical world, which means that it is challenging to apply them to an online context (cf. Koops 2012a, p. 42 and Koops 2013, p. 663-664). The legislature has to date not provided guidance as to how to apply them in the digital world. However, to a certain degree the factors can be applied to the digital context analogically, as detailed below.

The first factor, namely the *duration* of observation, can be applied in a digital world given that behaviours on the Internet can be observed for a specific period of time.

The second factor of the *place* from which a person's online behaviours are visible can also be applied to the Internet. For example, Dutch legislative history mentions that observing an individual visiting a brothel is a

41 See art. 126g DCCP. See also Corstens & Borgers (2014, p. 508) with regard to the legal basis in the DCCP for the application of the investigative method of observation in the physical world.

42 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 26-27.

43 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 26-27. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 7, p. 46.

44 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 26-27.

more intrusive investigative activity than observing an individual walking down the street.[45] Similarly, in an online context, observing the online conversations of individuals on a chat service designed for conversations of a sexual nature may be more privacy sensitive than observing the online behaviours of individuals on a chat service that aims to bring hobbyists of Lego together.

The third factor, namely the *intensity* of the investigative method, may relate in a digital context to the amount and diversity of the information that is gathered (cf. Oerlemans & Koops 2012, p. 45). For example, law enforcement officials can simultaneously observe an individual's behaviours on three different publicly accessible sources, such as Twitter account, a chat channel, and an online forum.

The fourth factor of the *frequency* of the observation of the behaviours of individuals can also be applied in an online context. For example, law enforcement officials can observe the behaviours of individuals on social media at regular intervals.

It remains unclear how the fifth factor of *using a technical device* can be applied in an online context. One can question whether utilising a computer with an internet connection to conduct online monitoring qualifies as using a 'technical device'. The use of an automated system that 'monitors' an individual's behaviours and sends frequent updates to a law enforcement official could possibly be interpreted as a technical device.

The interpretation of these five factors by analogy provides some guidance for the manner in which the investigative method is applied. However, it is unclear whether these factors are indeed adequately 'translated' to an online context and in which manner they are interpreted by the Dutch Police and Public Prosecution Service in practice. The articulated factors in legislative history are abstract and leave ample room for interpretation by law enforcement officials and public prosecutors. Furthermore, it is possible that other factors, which are specifically related to (features of) (privacy on) the Internet should be involved in determining whether not a particular application of this method is systematic. This requires consideration by the legislator.

C Case law

As explained in subsection 5.1.3, no case law is available that specifically deals with the legal basis for observation as an investigative method in an online context. The only case law that is available regards the use of observation as an investigative method in the physical world. However, even this case law is highly divergent as to the questions of when observation in the physical world becomes systematic and the use of the special investigative

45 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1997/98, 25 403, no. 7, p. 47.

power for systematic observation is thus required.[46] The case law simply repeats relevant parts of legislative history and does not provide further information regarding the application of the special investigative power in an online context, besides what can be deduced from the particular facts of a case.

D Public guidelines

The Guideline for Special Investigative Powers only specifies the manner in which the special investigative power for the systematic observation of the behaviours of individuals applies in the physical world.[47] It does not provide concrete information as to when application of the investigative method becomes systematic in nature, even in the physical world. Therefore, the guideline also does not provide clarification with regard to the difference between systematic and non-systematic application of observation in an online context.

5.2.4 Section conclusion

The foreseeability of the Dutch legal framework in criminal procedural law with regard to the gathering of publicly available information can be assessed using the analysis conducted in subsections 5.2.1 to 5.2.3. The results of this analysis are presented below.

The investigative method of the manual gathering of publicly available online information is not regulated in detail in Dutch criminal procedural law. Data protection regulations restrict the investigative method, but not in a concrete manner. In addition, legislative history indicates that a special investigative power is applicable when the investigative method is applied systematically. It is not clear, however, what the systematic gathering of online information entails and which special investigative power should be applicable. For that reason, the legal basis for this investigative method is considered *not foreseeable*.

With regard to the automated gathering of publicly available online information, no detailed regulations exist in Dutch law. The examined legislative history clearly has a different investigative method in mind than the current use of automated online data collection systems. Data protection regulations also provide no concrete interpretation of how these regulations apply for the automated gathering of publicly available online data. Given the absence of an indication of the scope of the investigative method in Dutch law and the manner it is applied, the legal basis for this investigative method is considered *not foreseeable*.

---

46 See, e.g., HR 29 March 2005, ECLI:NL:HR:2005:AS2752, HR 12 October 2010, ECLI:NL:HR:2010:BM4211 and Rb. Court of Limburg, 6 November 2013, ECLI:NL:RBLIM:2013:8519.

47 See section 2.2 of the Guideline for Special Investigative Powers.

The observation of the online behaviours of individuals can be based on art. 3 of the Dutch Police Act or the special investigative power for systematic observation. Statutory law, legislative history, and case law provide an indication of the scope of and the manner in which the investigative method is applied in the physical world. However, the five factors provided in legislative history for determining when observation becomes systematic were originally developed for observation in the physical world. Due to the lack of further guidance in case law or applicable guidelines, it remains unclear how these five factors are should be applied in an online context. The interpretation of these factors is currently at the discretion of law enforcement officials, who hopefully consult public prosecutors as to whether using the special investigative power for systematic observation is appropriate (cf. Oerlemans & Koops 2012, p. 46). Therefore, I conclude that the legal basis for the investigative method of observing the online behaviours of an individual is *not foreseeable*.

5.3 Quality of the law

Under the umbrella of the normative requirement regarding the quality of the law, the ECtHR can specify not only the level of detail required for the description of a power but also the minimum procedural safeguards that must be implemented vis-à-vis a particular method that interferes with the right to privacy. The detail that the ECtHR requires in the law and procedural safeguards depends on the gravity of the privacy interference that takes place.[48] This 'scale of gravity for privacy interferences' with regard to the gathering of publicly available online information is illustrated in Figure 5.1.

48 See subsection 3.2.2 under C.

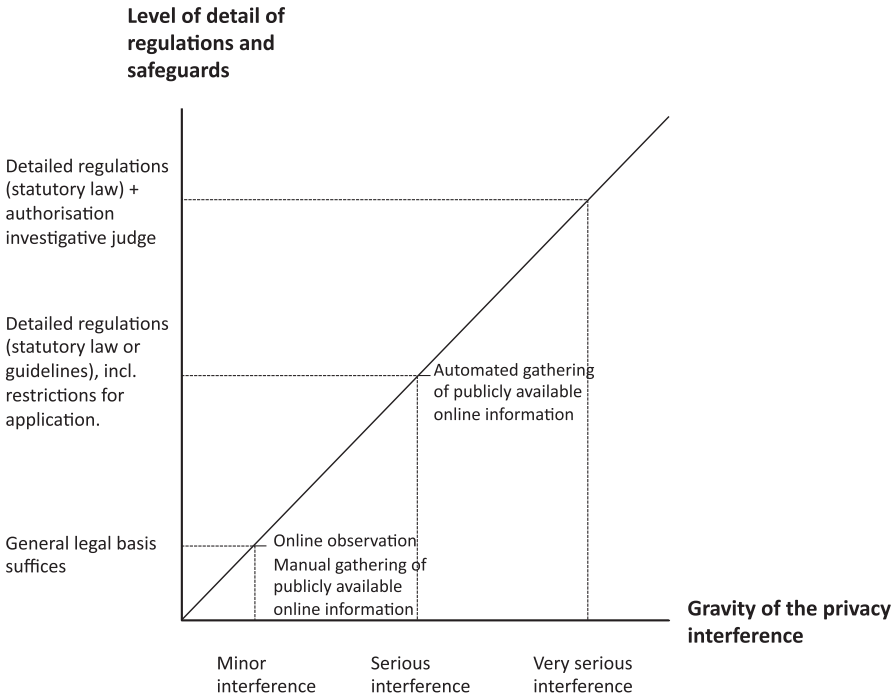

Figure 5.1: The scale of gravity for privacy interferences regarding the gathering of publicly available online information.

Figure 5.1 illustrates how it is likely that the ECtHR will not view the gathering of publicly available online information as a privacy infringing activity that merits detailed regulations in statutory law with stringent procedural safeguards. An important factor is that the information is publicly available to anyone and individuals can therefore expect that anyone, including law enforcement officials, can gather the information in a criminal investigation. However, data protection regulations restrict the evidence-gathering activity and require a minimum of protection to the individuals involved. In addition, the privacy interference is more serious when technologically advanced data collection systems are used, such as when publicly available online information is gathered automatically. In those circumstances, detailed regulations with procedural safeguards are desired as part of the quality of the law requirement.[49] Given the scale it deploys in case law, it may be expected that the ECtHR will also take this point of view. Of course, even if the ECtHR were not to set higher standards in this regard, the Dutch legal framework can require more detailed regulations with procedural safeguards for the different types of information gathering, based on higher standards derived from Dutch law.

49 See section 4.1 of chapter 4.

Remember that in the Netherlands, investigative methods that interfere with the rights and freedoms of individuals in a minor manner and do not threaten the integrity of criminal investigation can be based upon art. 3 of the Dutch Police Act.[50] Art. 3 of the Dutch Police Act does not require permission of a certain authority and does not restrict the application investigative method to criminal investigations with regard to certain crimes. Recently, the Dutch Supreme Court reaffirmed this interpretation of the criminal procedural legality principle in relation to the regulation of investigative methods.[51] On 1 July 2014, the Supreme Court decided that law enforcement authorities can send 'stealth text messages' (text messages that an individual receives, but cannot see) in order to localise an individual.[52] The text messages are sent while the individual is under surveillance by use of a wiretap. The Supreme Court reasoned that these stealth messages can be sent to a mobile phone of an individual based on art. 3 of the Dutch Police Act, insofar – depending duration, intensity, and frequency of the application of the investigative method – law enforcement officials do not acquire a more or less complete picture of certain aspects of an individual's life. The Dutch Supreme Court did not further specify at which point the application of a special investigative power is merited. Using the same reasoning, the Supreme Court also decided that law enforcement officials can use a so-called IMSI-catcher (a device that registers connecting cell phones by acting as a cell phone antenna) based on art. 3 of the Dutch Police Act, in order to track individuals.[53]

These judgements can be critiqued in the sense that they affect the required quality of the law for the regulation of investigative methods.[54] The main problem is that Dutch law enforcement authorities were not clear beforehand about their policy concerning the use of stealth messages to localise individuals. According to an *internal* guideline, the use of stealth messages must be mentioned in a police report and a public prosecutor must

50 See the introduction of this chapter.

51 See HR 1 July 2014, ECLI:NL:HR:2014:1563 and ECLI:NL:HR:2014:1569 and HR 1 July 2014, ECLI:NL:HR:2014:1562.

52 HR 1 July 2014, ECLI:NL:HR:2014:1563 and ECLI:NL:HR:2014:1569.

53 See also HR 1 July 2014, ECLI:NL:HR:2014:1562, *NBSTRAF* 2014/206, m. nt. C.J.A. de Bruijn. The Supreme Court took into consideration the circumstances at hand using (1) the factors mentioned above, (2) the fact that the investigative method is mentioned in a police report, (3) the fact that a public prosecutor ordered the application of the investigative method, and (4) the fact the special investigative powers of wiretapping and systematic observation were applied.

54 See most notably Borgers 2015 and HR 1 July 2014, ECLI:NL:HR:2014:1562, NJ 2015/115, m.nt. P.H.P.H.M.C. van Kempen.

authorize the investigative method.[55] Such a policy should have been public beforehand and the application of the investigative method should be described in a police report. As explained before[56], it is essential for the rule of law that individuals know under which conditions and in which manner investigative methods are applied by law enforcement officials, even when they (arguably) interfere with the right to privacy in only a minor manner.[57] It becomes even more essential where there is doubt that a general legal basis such as art. 3 of the Dutch Police Act is sufficient and that the investigative method rather requires the application of a special investigative power. When a policy for investigative methods is public, lawyers can object to the practice at trial and members of parliament can ask questions or take action by suggesting legislation for use of the investigative method. The Dutch Supreme Court could have been more critical about the secrecy surrounding the use of stealth text messages as an investigative method.[58] Hopefully, the practice of Dutch law enforcement authorities regarding the use of stealth text messages and IMSI catchers in the past, is not a harbinger of the use of digital investigative methods by law enforcement authorities that are at the border of interfering with the rights and freedoms of individuals in "*more than a minor manner*".

Hereinafter, the quality of the Dutch legal framework with regard to the identified categories of gathering publicly available online information as an investigative method is compared to the desired quality of the law as determined in chapter 4 for this method in subsections 5.3.1 to 5.3.3. Subsection 5.3.4 then presents conclusions regarding the adequacy of the quality of the Dutch legal framework for the digital investigative method.

55 See J.J. Oerlemans, 'Onduidelijkheid over de inzet van 'stealth smsjes' in opsporingsonderzoeken', *Computerrecht* 2013/217. See also the answers to parliamentary questions by Berndsen-Jansen and Schouw on 17 September 2013, about the article that law enforcement authorities unlawfully send stealth text messages to mobile phones to track suspect and the answers to parliamentary questions by Gesthuizen, Kooiman, Berndsen-Jansen and Schouw on 9 May 2014, about the use of stealth messages by law enforcement authorities for investigative purposes.

56 See subsection 3.2.2.

57 See similarly Borgers 2015, who argues that these kinds of judgments can lead to legal uncertainty for both law enforcement officials and citizens involved.

58 See also HR 1 July 2014, ECLI:NL:HR:2014:1562, NJ 2015/115, m.nt. P.H.P.H.M.C. van Kempen. Borgers (2015) suggests that the Surpreme Court could also prescribe more stringent conditions, such as authorisation of a public prosecutor (instead of taking it into account as a condition to decide on the legitimacy of the investigative method based on art. 3 of the Dutch Police Act).

5.3.1 Manual gathering of publicly available online information

The analysis in section 4.1 determined that the privacy interference that takes place when law enforcement officials manually gather publicly available online information is not likely to be considered as a serious interference by the ECtHR. As the information is publicly available, individuals can expect that anyone, including a law enforcement official, can gather the information in a criminal investigation. However, a graver interference with the right to privacy as defined in art. 8 ECHR takes place when personal information is stored in police systems. As part of the desired quality of the law, it was suggested in section 4.1 that data protection regulations should apply to the mere processing of personal information. Whereas the ECtHR only regards the systematic gathering and storage of information from publicly available sources as an interference of art. 8 ECHR, I argued that it is more appropriate to apply EU data protection regulations as soon as publicly available (online) information is processed by law enforcement authorities. Processing personal information about individuals does not require the systematic gathering and the storage of information in a police system. For example, a manual search of information about an individual on the Internet triggers data protection regulations. In this way, the right to privacy of individuals is protected sooner than the ECtHR currently requires.

Application to the Dutch legal framework
The Dutch legislator appears to assume that art. 3 of the Dutch Police Act suffices as a legal basis (in combination with data protection principles), insofar as the investigative method is not applied in a 'systematic' manner. When the investigative method is utilised systematically, a special investigative power should be applied.

However, the Dutch legislature has failed to clarify what the 'systematic gathering of online information' entails and which special investigative power is applicable in that case. Whether a digital investigative method interferes with the right to privacy in a minor manner is furthermore difficult to determine.

On the one hand, the amount of information about individuals that is available on the Internet has greatly increased since the legal basis for the investigative method was created in Dutch law back in 1999 (cf. Koops 2013, p. 663). This indicates the investigative method should nowadays *per se* be considered as more intrusive.

On the other hand, the gathering of publicly available information from the Internet about individuals involved in a criminal case is part of regular police work and is similar to gathering information from physical 'open sources' that law enforcement officials use to support criminal investigations. As the analysis of this investigative method in light of art. 8 ECHR has shown, the ECtHR will factor an individuals' public disclosure of information and public availability into its consideration. These factors will likely diminish the gravity of the privacy interference that takes place, since it influences the reasonable expectation of privacy of individuals.

However, it is worrisome that some law enforcement officials seem to believe that publicly available online information can be gathered infinitely (see Koops 2012a, p. 32 and Lodder et al. 2014, p. 72-73).[59] In this respect, the bad track record of Dutch law enforcement authorities regarding upholding the Police Files Act is also troubling.[60] Restrictions to evidence-gathering activities are only meaningful in terms of the quality of the law, insofar as the restrictions are effectively enforced.[61]

5.3.2 Automated gathering of publicly available online information

The ECtHR has shown in case law that it is critical of law enforcement activities that involve a pre-emptive collection of personal information for law enforcement purposes. When publicly available online information is automatically gathered using data collection systems, a more serious interference with the right to privacy as defined in art. 8 ECHR takes place. In addition, the use a 'technically sophisticated system' and the fact that information is processed about individuals who are not suspected of a crime indicate that the ECtHR will set stricter standards in this context. In section 4.1.3, I argued that the result of the balancing test that should be conducted in this regard, also in terms of the requirements of a legitimate aim and the necessity of the method in a democratic society should be reflected in detailed regulations for the investigative method. Existing data protection regulations can aid in both creating these new regulations and determining further adequate safeguards.[62]

Application to the Dutch legal framework

In the Netherlands, no detailed regulations are available for the investigative method of automated gathering of publicly available information. Considering the intrusiveness of this method, one can argue that it should be regulated as a special investigative power. However, automated data col-

59 See also Harry Lensink & Gerard Janssen, 'Plaats delict: social media', *Vrij Nederland*, 18 April 2014. Available at: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Plaats-delict-social-media.htm (last visited on 10 June 2015).

60 See, e.g., the following press releases of the Dutch Data Protection Authority: 'Regionale politiekorpsen niet toegerust op nieuwe eisen gegevensbescherming CBP zal vervolgonderzoek doen bij individuele korpsen', 14 October 2008, 'Verwerking persoonsgegevens door regionale politiekorpsen Vervolgonderzoek CBP naar functioneren politie infodesks', 16 July 2009, 'Politie en opsporingsdiensten verzuimen privacyaudit uit te voeren', 19 July 2011 and Bart de Koning, 'Nieuws: de politie blijkt op grote schaal de wet te overtreden', *De Correspondent*, 8 December 2015. Available at: https://decorrespondent.nl/3734/Nieuws-de-politie-blijkt-op-grote-schaal-de-wet-te-overtreden/446202963008-90777447 (last visited on 4 January 2016).

61 In that respect, see also ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 250-301. Although this case regards the more privacy-intrusive investigative method of the interception of communications, it makes it clear that the ECtHR finds it important that the safeguards against abuse are effective and thus applied in practice.

62 See the analysis in subsection 4.1.3 under B.

lection systems can also be used for public order purposes. A separate bill that regulates the general use of automated data collection systems by law enforcement officials appears more appropriate.

The Dutch legislature currently has no plans to create detailed regulations that restrict the automated gathering of publicly available online information. As mentioned in subsection 5.1.2, the use of the 'iColumbo' automated online data collection system meets the Dutch Police Files Act's requirements according to the Dutch legislator.[63] This point of view is remarkable, since the cited report by Koops et al. *did not* state that the system is in line with data protection regulations. The report only stipulated the conditions that the system has to comply with in order to meet data protection requirements (Koops et al. 2012a, p. 41-43). Serious concerns may thus be raised as to whether the Dutch regulations for automated data collection systems meet the desirable quality of the law.

The need for more detailed regulations for the automated gathering of publicly available online information for law enforcement purposes is also supported by the cases of *Digital Rights Ireland v. Ireland* and *Seitlinger, Tschohl et al. v. Kärtner Landsregierung* (hereinafter: *Digital Rights Ireland* and *Seitlinger*) of the Court of Justice of the European Union (hereinafter: CJEU) (cf. Lodder & Schuilenburg 2016, p. 152).[64] Case law of the CJEU is directly applicable to the Dutch legal framework and its decisions must be incorporated into Dutch law. Both cases are therefore briefly examined.

On 8 April 2014, the CJEU decided in the landmark cases of *Digital Rights Ireland* and *Seitlinger* that retaining telecommunication data is a form of personal data processing that interferes with the right to respect for private life and the right to data protection as defined in art. 7 and 8 of the CFR.[65]

In its decision, the CJEU refers to case law of the ECHR regarding interferences with the right to privacy that take place when personal data is stored in police systems.[66] The CJEU additionally takes into consideration that personal information is also retained about individuals who are not suspected of a crime (cf. Boehm & Cole 2014, p. 35-38).[67]

In the cases of *Digital Rights Ireland* and *Seitlinger*, the Advocate General also argued that the retention of personal data may also harm aspects of the rights to freedom of expression and information. The reason for this

63 See the memorandum 'Freedom and safety in the digital society. An agenda for the future' of 14 December 2013, 26 643, no. 298, p. 12. See also subsection 5.1.2.

64 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*).

65 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 29.

66 See CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 35 referring to ECHR 26 March 1987, *Leander v. Sweden*, appl. no. 9248/81, § 48, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 46, ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 79.

67 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 57-59. See also subsection 4.4.1.

is that the knowledge that a government continuously gathers information about its citizens may stifle individuals' behaviours.[68] This so-called 'chilling effect' often accompanies surveillance measures. The CJEU did not further address the interference with the freedom of expression, because it deemed doing so 'unnecessary' after its extensive analyses of art. 7 and 8 CFR.[69] However, in my view the chilling effect is indeed a factor that needs to be taken into consideration when regulating law enforcement authorities' usage of automated data collection systems.

Similar to the ECtHR, the CJEU carefully scrutinises whether the quality of the law for the regulation of investigative methods is proportionate considering the aim that is being pursued. In doing so, it notes that domestic regulations of data retention measures must impose a minimum of legislated safeguards to effectively protect personal data from both abuse and unlawful access to data by law enforcement authorities.[70] The CJEU finds that regulations must specifically consider three aspects, namely: (1) the vast quantity of data that is stored as a result of the Data retention directive, (2) the sensitive nature of that data, and (3) the risk of unlawful access to that data.[71] Interestingly, the CJEU remarks that "*the need for such safeguards is all the greater where, (…), personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data*".[72] This comment supports the view that detailed regulations should restrict the use of automated data collection systems by law enforcement officials.

5.3.3 Observation of online behaviours of individuals

An interference with the right to respect for private life takes place when law enforcement officials observe online public behaviours of individuals. The investigative method can likely be placed at the low end of the scale of gravity for privacy interferences, given that these online behaviours can be observed by anyone. However, in its case law, the ECtHR has developed the following factors for determining the gravity of the privacy interference and the quality of the law regulating it: (1) the nature, scope, and duration of the surveillance measures; (2) the grounds required for ordering them; (3) the authorities competent to permit, carry out, and supervise the measures;

68 AG Opinion to CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 53.

69 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 70.

70 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 54. These safeguards must be implemented in addition to the requirements of accessible and foreseeable law. The CJEU also refers to ECtHR case law, such as *S. and Marper v. The United Kingdom* and *Rotaru v. Romania*.

71 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 66.

72 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 55.

and (4) the kind of remedy provided by the national law for violations.[73] If contracting States of the ECtHR are to comply with these factors in their domestic legal frameworks, it appears logical that they regulate the investigative method in detail, incorporating these factors therein.[74]

Application to the Dutch legal framework

As explained in sections 5.1 and 5.2, the observation of the behaviours of individuals in public is viewed as a privacy-infringing activity in the Netherlands. However, the detailed legal basis with procedural safeguards is applicable in the DCCP only when the observation becomes systematic in nature. In my view, it is not necessary to require more stringent procedural safeguards in connection with systematic online observation (as opposed to systematic offline observation), such as the involvement of an investigative judge. The current requirement for a public prosecutor's order for the systematic observation of online behaviours of individuals is appropriate.

If the factors that the ECtHR already considers when it determines the gravity of a privacy interference and the quality of the law are taken into account, a detailed legal basis in statutory law appears appropriate for both the non-systematic and systematic application of this investigative method. The details concerning how individuals are observed in an online context could be regulated in a guideline for the Public Prosecution Service. The need for a guideline that explains in more concrete terms when the special investigative power to systematically observe individuals' (online) behaviours will be required is clear. The most recent study (2004) regarding the application of this investigative method concluded that it is unclear for law enforcement officials when the application of the special investigative power for systematic observation is required for this method even in the physical world (see Beijer et al. 2004, p. 36 and 59). With a lack of case law and direction in guidelines for law enforcement officials, I do not expect the *online* application of the investigative method to be any clearer in practice.

5.3.4 Section conclusion

The results of the analysis in subsections 5.3.1 to 5.3.3 with regard to the adequacy of the quality of the law of the Dutch legal framework conducted presented below.

The manual gathering of publicly available online information by law enforcement authorities is considered a privacy-infringing activity in the Netherlands. The Dutch regulations *meet the desired quality of the law*, since the investigative method is restricted by data protection regulations. However, Dutch law enforcement authorities must exert more effort to ensure

73 The 'kind of remedy' refers to a remedy for procedural defects in the investigation by law enforcement authorities. This criterion does not relate to art. 8 ECHR or the regulation of the investigative method itself and is therefore not further considered.

74 See subsection 4.1.2 under C and subsection 4.1.3 under C.

that data protection regulations effectively restrict evidence-gathering activities. At the moment, law enforcement authorities do not sufficiently apply these regulations.

The automated gathering of publicly available online information is not regulated in detail in the Netherlands. Case law of both the ECtHR and CJEU indicates that each court will carefully compare the need to collect information with the aim that is being pursued by gathering the data. The result of that comparison must be reflected in detailed regulations that concretely interpret requirements arising from data protection regulations. The Dutch Police Files Act is not tailored to this investigative method. As a result, the legal basis for the automated gathering of publicly available online information *does not meet the desired quality of the law* requirements

The observation of the online behaviours of individuals is considered a privacy-infringing activity in the Netherlands. A detailed provision in criminal procedural law, with the specific procedural safeguard of an order being required from a public prosecutor is only applicable when the investigative method is applied systematically. The Dutch legal framework with regard to the investigative method of the observation of the online behaviours *does not meet the desired quality of the law* requirements, due to ambiguity with regard to the question of when (online) observation as an investigative method becomes systematic in nature. A guideline should more concretely detail when a special investigative power is required for such observation.

5.4 Improving the legal framework

This section discusses how the DCCP can be improved in order to provide an adequate legal framework for the regulation of the investigative method of gathering publicly available online information. A legal framework is considered adequate when (1) it is accessible, (2) it is foreseeable, and (3) the desired quality of the law requirements are met. The results of the analysis regarding these normative requirements are summarised in Table 5.1.

Normative requirement	**Manual gathering of publicly available online information**	**Automated gathering of publicly available online information**	**Observing the online behaviours of individuals**
Accessible	✓	✓	✓
Foreseeable	✗	✗	✗
Meets the desirable quality of the law	✓	✗	✗

Table 5.1: Representation of the research results from sections 5.1 to 5.3 (✓ = adequate, ✗ = not adequate).

These research results are the basis for making suggestions for improving how the Dutch legal framework regulates each category of gathering publicly available online information. The improvements related to each investigative method are presented in the following subsections.

5.4.1 Manual gathering of publicly available online information

The Dutch legal framework for the manual gathering of publicly available online information is not considered foreseeable, due to its ambiguity with regard to how data protection regulations must be interpreted concretely in the context of the investigative method. In addition, the Dutch legislature has previously made a confusing statement that a special investigative power is required for the systematic information gathering of online information.[75]

Taking the desired quality of the law for this investigative method into account, I argued above that the general legal basis in art. 3 of the Dutch Police Act may suffice for the investigative method, in combination with data protection regulations. However, the data protection regulations themselves are not taken into sufficient consideration by Dutch law enforcement authorities and need to be applied more concretely.

In order to improve the investigative method's foreseeability and the quality of the law, it is recommended to create a guideline for the manual gathering of publicly available online information (*Recommendation 1*).[76] Dutch law enforcement officials can and should be provided with more guidance from the Dutch legislator or Public Prosecution Service with regard to the question as to how the manual gathering of publicly online information should be restricted. The guideline for 'internet investigations' prepared by municipal investigators can be used as an example in this regard.[77] Most notably, this guideline requires investigators to (1) consider whether it is necessary to look for information about the individual online and perform a proportionality test in relation to the crime at hand, (2)

75 In 2014, the Dutch Ministry of Security and Justice proposed a new special investigative power that allows law enforcement officials to 'systematically download online data' in criminal investigations of every crime, insofar as a legal order is obtained from a public prosecutor. See the discussion document regarding special investigative powers (6 June 2014), p. 59-60. Available at: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/herziening-van-het-wetboek-van-strafvordering. However, in his letter of 30 September 2015 on the modernisation of the DCCP, the Dutch Minister of Security and Justice suddenly stated that the Dutch national police no longer desired a new special investigative power for the 'systematic collection of personal data from the Internet'. See the letter of 30 September 2015 regarding the modernisation of the DCCP, p. 88. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (last visited on 3 May 2016). Since then, no legislative initiatives have been made to improve Dutch legislation regarding the gathering of publicly available online information.

76 Alternatively, the existing Guideline for Special investigative Powers can be amended to incorporate the investigative method.

77 See 'Protocol internetonderzoek door gemeenten'. Available at: https://cbpweb.nl/sites/default/files/atoms/files/protocol_internetonderzoek_door_gemeenten.pdf. The Dutch Data Protection Authority found the guideline appropriate in light of data protection regulations. See 'Besluit internetonderzoek door gemeenten', 17 April 2015. Available at: https://cbpweb.nl/nl/nieuws/besluit-internetonderzoek-door-gemeenten (last visited on 17 September 2015).

develop a search strategy – and thereby a basis for the police report – that includes which combination of key words and online sources they will use in their investigation, and (3) provide a police report that states the results of their online investigation. The guideline also restricts the investigative method in a concrete manner by posing a time limit on the gathering of publicly available information, after which law enforcement officials must obtain authorisation from a higher-ranking law enforcement official if they feel it is necessary to continue their search.

5.4.2 Automated gathering of publicly available online information

The legal basis for applying the automated gathering of publicly available online information is not 'in accordance with the law', since the normative requirements of foreseeability and the quality of the law requirements are not met. Detailed regulations should restrict this privacy-intrusive investigative method and protect the individuals involved. Case law of both the ECtHR and CJEU requires that States carefully test the necessity to collect information and the aim that is pursued by gathering that data.

The result of this test should be reflected in detailed regulations that minimise the risk that the data will be abused or unlawfully accessed and used. The Police Files Act is not tailored to this investigative method. The creation of detailed regulations in statutory law would force the Dutch legislature to think about the necessity and conditions for using automated data collection systems. These bodies should also engage in a broader debate about the use of commercial online data collection services by law enforcement authorities.

The detailed regulations themselves may be comparable to legislation that is already in place for CCTV camera surveillance in public places (*Recommendation 2*). It is likely that automated information-gathering systems will be used for public order purposes, as well as for gathering evidence in criminal investigations. The detailed regulations should at least specify (1) for which purposes and which crimes automated data collection systems can be utilised, (2) the retention period for the data, (3) the organisational and technical security measures for securing information, (4) which organisations individuals should approach should they wish to invoke their right to access and correct data, and (5) which remedies are available to the individuals involved when errors occur.

5.4.3 Observation of online behaviours of individuals

In the Netherlands, the observation of the online behaviours of individuals is based on either (1) the statutory duty of the law enforcement officials and public prosecutors to investigate crimes or (2) the special investigative power for systematic observation. However, it is currently unclear when the observation of individuals becomes 'systematic' in nature and hence when the special investigative power for systematic observation is required

as a legal basis. The factors with the accompanying explanation provided in legislative history in 1999, appear to be outdated. Whether the use of the special investigative power for systematic observation is appropriate is currently left to the discretion of law enforcement officials, who hopefully consult with public prosecutors (cf. Oerlemans & Koops 2012, p. 46). More clarity about the application of the investigative method is required for both law enforcement officials and the individuals involved.

The Dutch legislator or Public Prosecution Service should create more detailed regulations in a guideline that specifies under which conditions this investigative method can be applied (*Recommendation 3*). This guideline could interpret the factors provided in legislative history in an online context and thus indicate more concretely when the application of the special investigative power for systematic observation is appropriate. The Dutch legislator can also consider amending the special investigative power for systematic observation and specifying a time limit that defines when observation becomes systematic in nature. However, a downside of such a condition would be that a time limit does not consider the fact that this investigative method can be intrusive to the individuals involved when their online behaviours are observed from multiple sources or in particularly sensitive online contexts.

5.5 Chapter conclusion

The aim of this chapter was to determine how Dutch criminal procedural law should be improved to adequately regulate the investigative method of gathering publicly available online information (RQ 4a). To answer the research question, the Dutch legal framework regulating all three categories of the investigative method was investigated with regard to (1) accessibility, (2) foreseeability, and (3) the quality of the law.

In this study, the gathering of publicly available online information is subdivided into (1) the manual gathering of publicly available online information, (2) the automated gathering of publicly available online information, and (3) the observation of online behaviours. Law enforcement authorities have traditionally viewed the gathering of information from these 'open sources' as investigative methods that do not require detailed regulation in the form of 'special investigative powers' in criminal procedural law. However, a much larger amount of more diverse information is now publicly available on the Internet. The analysis in subsection 4.1.3 has shown that this investigative method – and especially the use of technologically advanced systems to collect and process personal data – should be subject to detailed regulations.

Subsection 5.5.1 summarises the results of the adequacy of the Dutch regulations for the investigative method in terms of the three normative requirements. The corresponding recommendations are presented in subsection 5.5.2.

5.5.1 Summary of conclusions

In section 5.1, an analysis regarding the accessibility of the legal basis for the investigative method was conducted. That analysis showed that Dutch law provides an adequate indication of the applicable regulations for the manual gathering of publicly available online information, the automated gathering of publicly available online information, and the observation of online behaviours.

The analysis in section 5.2 showed that none of the categories of gathering publicly available online information is regulated in a foreseeable manner in Dutch law. Data protection principles restrict the manual and automated gathering of publicly available online information. However, the way in which these data protection regulations restrict these particular investigative methods is unclear. In addition, the examples mentioned in legislative history, which includes the explanatory memorandum to the Computer Crime Act II of 1999, appear outdated. Today a larger amount of more diverse information about individuals is publicly available on the Internet. The Dutch legislature or Public Prosecution Service should indicate the scope of the manual gathering of publicly available online information more clearly in statutory law or guidelines. In addition, the Dutch legislature or Public Prosecution Service should explain how the factors provided in legislative history to determine when the investigative method observation becomes systematic in nature, apply in an online context and if necessary, design new determining factors tailor made for the online context. Finally, the Dutch legislature should discuss the desirability of automated data collection systems that are used to gather publicly available online information for law enforcement purposes. The scope of this investigative method and the manner in which it is used should be restricted in detailed regulations in statutory law.

The analysis in section 5.3 showed that only the manual gathering of publicly available online information meets the desired quality of the law. However, in the context of this method, Dutch law enforcement authorities must exert more effort to ensure that data protection regulations effectively restrict evidence-gathering activities. The current situation is that law enforcement authorities do not sufficiently apply these regulations. In order to meet the desired quality of the law for the automated gathering of publicly available online information, detailed regulations that reflect requirements from data protection regulations must be created. The observation of the online behaviours of individuals does not meet the desired quality of the law, due to ambiguity with regard to when (online) observation as an investigative method becomes systematic in nature. A guideline should detail more concretely when the special investigative power is required for observing the online behaviours of individuals. This reflection is continued in subsection 5.5.2.

5.5.2 Recommendations

Section 5.4 provided three recommendations to improve the Dutch legal framework for the gathering of publicly available online information as an investigative method. These recommendations followed the analysis of the adequacy of the Dutch legal framework based on the three normative requirements in section 5.1 to 5.3. The recommendations are as follows.

1. The Dutch legislator or Dutch Public Prosecution Service should create a guideline for the manual gathering of publicly available online information. This guideline can specify the scope of the investigative method, explain the manner in which the method should be applied in practice, and restrict the investigative method by specifying how the data protection regulations should be concretely fulfilled.
2. The Dutch legislator should create detailed regulations (statutory law) for the use of the automated gathering of publicly available online information as an investigative method that are comparable to the existing regulations for using CCTV cameras. These detailed regulations should also specify how data protection regulations should be concretely fulfilled.
3. The Dutch legislator or Public Prosecution Service should create more detailed regulations for the observation of online behaviours of individuals. A guideline could specify more explicitly under which conditions this investigative method can be applied and when the application should be considered systematic.

6 Issuing data production orders to online service providers

This chapter aims to answer the fourth research question with regard to data production orders that are issued to online service providers (RQ 4b): *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate the issuing of data production orders to online service providers?* Four types of data production orders are distinguished that can be issued to online service providers. These are as follows: (1) subscriber data, (2) traffic data, (3) other data, and (4) content data.

To answer the research question, the investigative method is placed within the Dutch legal framework and further analysed to determine whether the normative requirements for the regulation of investigative methods from art. 8 ECHR are met. In chapter 3, the normative requirements were identified as follows: (1) accessibility, (2) foreseeability, and (3) the quality of the law.

Chapter 4 formulated the requirements for the regulation of different investigative methods based on art. 8 ECHR. The desired requirements for data production orders that are issued to online service providers are specifically formulated in subsection 4.2.3. The analysis has shown that detailed regulations for the investigative method are desired. The desired procedural safeguards differ by type of data, since the different types of data production orders interfere with the right to privacy in different manners. It must be noted here again that the point of departure is that the requirements that flow from art. 8 ECHR are minimum standards. Dutch criminal procedural law can impose a higher level of protection to the individuals involved.

Brief description of the Dutch legal framework for data production orders

At this juncture, it is helpful to explain the basics of the Dutch legal regime in relation to data production orders. In Dutch criminal procedural law, two regimes for data production orders are applicable.[1] In 2004, specific legislation was created in the DCCP for data production orders that law enforcement authorities could issue to public telecommunication and

1 Here it is worth noting that the special investigative powers that regulate data production orders must always be issued to gather data from persons, institutions, or companies, unless that third party discloses the data by himself (for example when reporting a crime to the police). Dutch law enforcement authorities are not allowed to request third parties to voluntarily disclose the data they hold without using the special investigative power that regulates the data production order (see HR 21 December 2010, ECLI:NL:HR:2010:BL7688). See also, J.J. Oerlemans, 'Vorderen van gegevens van Crimesite.nl', OerlemansBlog, 11 January 2011. Available at: https://oerlemansblog.weblog.leidenuniv.nl/2011/01/11/vorderen-van-gegevens/ (last visited on 10 October 2014).

financial service providers.[2] Shortly thereafter, in 2005, the Dutch legislature created a specific legal basis for data collection orders that can be sent to all other persons, institutions, and companies.[3] The legislation for data collection orders that are issued to telecommunication providers remained unchanged, except that the term 'telecommunication service provider' was amended to 'electronic communication service provider' in the data production order powers that are regulated as special investigative powers in the DCCP.[4] Thus within the two legal regimes that exist for data production orders in Dutch criminal procedural law, the first tier of data production orders is designed for electronic communication service providers, while the second tier applies to all other persons, institutions, and companies.[5] The Dutch regulations for data production orders are illustrated in Figure 6.1 by plotting them on the scale of gravity for privacy interferences and accompanying quality of the law that is derived from art. 8 ECHR.

2 The Act on Data Production Orders for Telecommunication Providers (Wet vorderen gegevens telecommunicatie, *Stb.* 2004, 105) and the Act on Data Production Orders for the Financial Sector (Wet vorderen gegevens van instellingen in de financiële sector, *Stb.* 2004, 109).

3 See the General Act on Data Production Orders (Wet vorderen gegevens *Stb*. 2005, 390). This act incorporated the Act on Data Production Orders for the Financial Sector (Wet vorderen gegevens van instellingen in de financiële sector, *Stb.* 2004, 109). The Parliamentary Inquiry Commission on Investigative Methods advised creating specific legislation for the collection of data stored by third parties in 1996 (*Kamerstukken II* 1995/96, 24 072, no. 11, p. 466). The proposed legislation for data collection powers with regard to telecommunication providers aimed to carry out this advice. See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2001/02, 28 059, no. 3 (explanatory Act on Data Production Orders for Telecommunication Providers), p. 3. In addition, the 'Commission Mevis' was requested to find out which investigative powers for data collection were appropriate in our 'information society' (Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij). The Dutch legislature eventually adopted most of the recommendations in the General Act on Data Production Orders.

4 See *Kamerstukken II* (Parliamentary Series Second Chamber) 2004/05, 26 671, no. 7, p. 43.

5 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 5. Issuing data production orders to individuals that have privileged information, such as lawyers, physicians, journalists, and clergymen, are only possible in limited circumstances. These regulations for privileged individuals are not further considered in this study.

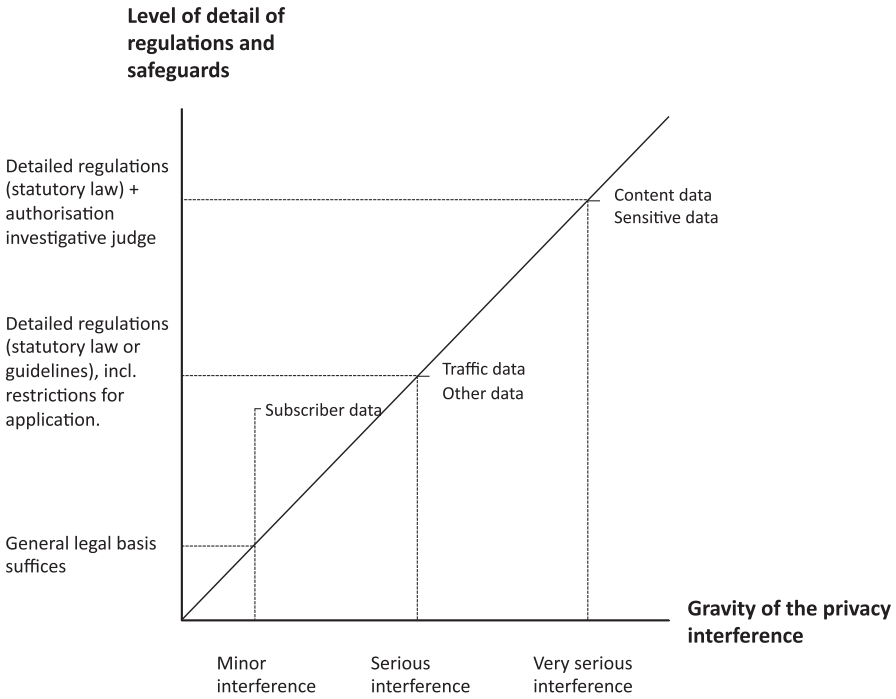

Figure 6.1: Scale of gravity and accompanying quality of the law for data production orders in Dutch criminal procedural law.

Figure 6.1 above illustrates how Dutch law differentiates between requirements for regulations for data production orders based on the privacy interferences that accompany the different types of data production orders.[6] The analysis in this chapter shows whether the current Dutch legal framework aligns with the desired requirements that were that were derived from art. 8 ECHR for this method in chapter 4.

Structure of the chapter

In this chapter, the three normative requirements are tested in separate sections, each of which discusses all four types of data production orders. To assess the accessibility and foreseeability of the Dutch legal framework with regard to the investigative methods, the same scheme of research is used as in chapter 5. That scheme entails examining the following four sources of

6 Figure 6.1 represents a simplified model of the Dutch legal framework. The quality of the law for data production orders also differs by their type of criminal investigations that are restricted to the seriousness of the offence. Furthermore, the special investigative powers in Dutch criminal procedural law with regard to 'future generated data' and 'data preservation orders' (as meant in art. 126ne DCCP and art. 126ni DCCP) are not examined in this chapter, because they are not distinguished as a relevant type of data production order in chapter 2.

law: (A) statutory law, (B) legislative history, (C) case law, and (D) public guidelines. Thereafter, the requirements for regulations extracted from art. 8 ECHR for this method are compared to the Dutch legal framework. Based on the results of the analyses, recommendations are provided to improve the Dutch legal framework.

Section 6.1 thus tests the *accessibility* of the legal basis for the investigative method in the Dutch legal framework. Section 6.2 examines to which extent the method is regulated in a *foreseeable* manner in the Netherlands. Section 6.3 analyses whether the Dutch legal framework meets the *desired quality of the law*. Based on the results of the analyses conducted in these sections, section 6.4 provides concrete proposals as to how Dutch criminal procedural law can be improved to adequately regulate data production orders that are issued to online service providers. Section 6.5 concludes the chapter by summarising its findings.

6.1 Accessibility

An accessible basis in law means that the individual involved has an adequate indication of which regulations apply to the use of investigative methods in a particular case.[7] Given the detailed regulations that have been created for data production orders in the Netherlands, it is expected that this normative requirement will be unproblematic for Dutch law.

Before proceeding, it is important to explain the relationship between accessibility and the dual regime for data production orders in the Dutch legal framework. The reason is that ambiguity exists with regard to the issue under which of the two regimes online service providers must be placed: are they electronic communication service providers or should they be considered an 'other company or institution'? Article 126la DCCP defines an 'electronic communication service provider' as follows:

"a commercially motivated person or company that provides a communication service with the aid of computers, or processes or stores data on behalf of its users for such a service"

This definition focuses on providing '*communication services*' with the aid of computers. As such, webmail-, social media-, forum-, and anonymising service providers can all be considered electronic communication service providers. However, it is unclear whether hosting and online storage providers should be considered electronic communication service providers as well (cf. Koops et al. 2012b, p. 42), as they do not necessarily provide 'communication services' for individuals.

7 See subsection 3.2.2 under A.

Nonetheless, it is likely that these online service providers also fall into the category of electronic communication service providers as defined in art. 126la DCCP. An argument for this can be found in legislative history. Art. 126la DCCP was introduced after the Dutch government ratified the Convention on Cybercrime. The explanatory memorandum to the convention explains that within that treaty, the term 'service providers' also relates to entities that store or process information on behalf of their customers.[8] At the same time, however, it also implies that these service providers must also provide communication services (cf. Koops et al. 2012b, p. 42). Many cloud storage and hosting providers also provide communication services. For example, they often enable users to share documents with other users. Most online service providers will therefore be considered electronic communication service providers as meant in art. 126la DCCP in practice.[9] In the case of other online service providers, law enforcement authorities cannot obtain data under the legal regime of data production orders for electronic communication service providers. Instead, they can use the legal regime of data production orders for all other persons, institutions, and companies.[10] It is therefore important to examine both legal regimes for the regulation of data production orders in Dutch law.

Subsections 6.1.1 to 6.1.4 examine the accessibility of each of the four types of data production orders. Subsection 6.1.5 then draws conclusions regarding the accessibility of the investigative method in Dutch law.

6.1.1 Subscriber data

The subscriber data category relates to subscriber data that is available from online service providers. As explained in section 2.2 of chapter 2, subscriber data can be used to identify a suspect in cybercrime investigations.

The accessibility of the legal basis for obtaining subscriber data is examined below using the aforementioned research scheme.

---

8 Explanatory memorandum Convention on Cybercrime, par. 27: *"Under (ii) of the definition, it is made clear that the term "service provider" also extends to those entities that store or otherwise process data on behalf of the persons mentioned under (i). Further, the term includes those entities that store or otherwise process data on behalf of the users of the services of those mentioned under (i). For example, under this definition, a service provider includes both services that provide hosting and caching services as well as services that provide a connection to a network. However, a mere provider of content (such as a person who contracts with a web hosting company to host his web site) is not intended to be covered by this definition if such content provider does not also offer communication or related data processing services."*

9 This is also confirmed in my dossier research.

10 See section 2.3 of the Guideline for Special Investigative Power. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 13-14

A Statutory law

Dutch criminal procedural law regulates a special investigative power that enables law enforcement officials to obtain subscriber data from electronic communication service providers. Art. 126na(1) DCCP reads as follows:

"In case of reasonable suspicion of a crime and insofar it is in the interest of the investigation, law enforcement officials can issue a data production order to enable the disclosure of name, address, postal code, place of residence, number, and type of service of a subscriber of a communication service (…)."

A second special investigative power enables law enforcement officials to obtain subscriber data from all other persons, institutions, and companies. Art. 126nc(1) DCCP reads as follows:

"In case of reasonable suspicion of a crime and insofar it is in the interest of the investigation law enforcement officials can issue a data production order concerning stored and identifiable personal data to those who reasonably qualify and do not process data for personal use."

The category of 'identifiable personal data' is listed in art. 126nc(2) DCCP. This provision reads as follows:

"Identifiable data is understood as:
a. name, address, place of living and postal address;
b. data of birth and gender;
c. administrative data;
d. insofar the information is obtained from a company, the location of data, as meant under a and b: name, address, postal address, type of business and location of its headquarters."

These two special investigative powers indicate that accessible regulations exist for the issuing data production orders concerning subscriber data to online service providers. As such, an accessible legal basis for issuing data production orders to online providers to obtain subscriber data is available in statutory law. It is notable that the second special investigative power to obtain subscriber data in art. 126nc DCCP includes of slightly different set of data.

B Legislative history

The explanatory memorandum to the Act on Data Production Orders for Telecommunications providers and the General Act on Data Production

Orders both specify what subscriber data entails.[11] An indication of the legal basis for issuing data production orders to online providers to obtain subscriber data is therefore available in legislative history.

C Case law

Case law indicates that law enforcement officials can obtain name and address information that is associated with an IP address from internet access providers by using the special investigative power to obtain subscriber data from electronic communication service providers.[12] This special investigative power is applied relatively often in criminal investigations that concern child pornography cases.[13]

The available case law shows that foreign law enforcement authorities frequently disseminate IP addresses that they find in their own domestic child pornography investigations to other law enforcement authorities. As explained in subsection 2.2.1, IP addresses are a powerful lead in cybercrime investigations and can enable law enforcement officials to obtain name and address data of the subscriber from an internet access provider.[14] This information can then lead the officials to the suspect's residential address, where they can perform a search (after obtaining the requisite warrant to do so). During this search, the officials can seize computers and interrogate people at the site. The digital evidence stored on the computers and the interrogation results may then provide evidence of the (cyber)crime that has been committed. Case law thus indicates that the special investigative power to obtain subscriber data from electronic communication service providers is relatively often applied to obtain subscriber data from online service providers. The available case law does not indicate that art. 126nc DCCP is applied to obtain subscriber data from online service providers.

11 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2001/02, 28 059, no. 3 (explanatory memorandum Act on Data Production Orders for Telecommunication Providers), p. 5-6 and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 7-8.

12 See, e.g., Rb. Amsterdam, 1 October 2009, ECLI:NL:RBAMS:2009:BK1564 Rb. Groningen, 20 May 2010, ECLI:NL:RBGRO:2010:BM5193, and Rb. Overijssel, 9 April 2013, ECLI:NL:RBOVE:2013:BZ6638.

13 See, e.g., Rb. Groningen, 22 October 2009, ECLI:NL:RBGRO:2009:BK1004, Rb. Noord-Nederland, 4 February 2013, ECLI:NL:RBNNE:2013:BZ9666, Rb. Noord-Holland, 10 September 2015, ECLI:NL:RBNHO:2015:8404, and Hof Den Haag, 17 November 2015, ECLI:NL:GHDHA:2015:3257.

14 This finding is also repeatedly mentioned in the explanatory memorandum of the amended Data Retention Act (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 537, no. 3, p. 5-7. Several cases are mentioned in the explanatory memorandum to emphasise the importance of the availability of IP addresses (coupled with subscriber data) to law enforcmeent authorities.

D Public guidelines

The Guideline for the Special Investigative Powers of the Public Prosecution Service of 2014 further details the regulations for data production orders that are issued to (tele)communication providers and other persons, institutions, and companies.[15] It focuses heavily on information that is available at public telecommunication service providers and does not explain which online service providers are considered electronic communications service providers.

However, the guideline does indicate that law enforcement officials can obtain 'other subscriber data' from online service providers, insofar as the first special investigative power to obtain subscriber from electronic communication providers does not provide the officials with the information they are seeking.[16] The guideline therefore further illustrates how the Dutch legal regime for data production orders works in criminal procedural law.

6.1.2 Traffic data

The category of traffic data consists of data that is generated by a computer system as part of a chain of communication. Traffic data can reveal information about communications, such as origin, destination, route, time, date, size, duration, and type of underlying service. Law enforcement officials can obtain valuable evidence by analysing network traffic data, which may aid them in locating individuals, identifying services that those individuals have used, and pinpointing computer users based on IP addresses.[17]

The accessibility of the legal basis for obtaining traffic data is examined below using the announced research scheme.

A Statutory law

Law enforcement officials can use the special investigative power in art. 126n(1) DCCP to obtain traffic data from electronic communication service providers.[18] Art. 126n(1) DCCP reads as follows:

"In case of reasonable suspicion of a crime as defined in art. 67(1) DCCP and insofar it is in the interest of the investigation, a public prosecutor can issue a data production order to obtain data regarding a subscriber of a communication service and the traffic data of communications regarding that user. The order can only regard data that is stipulated in lower regulations and can concern data, (a) which were processed during the issuing of the order or (b) which are processed after the issuing of the order."

15 See section 2.3 and section 2.10 of the Guideline for the Special Investigative Powers.
16 Based on art. 126ng(1) DCCP jo art. 126nc DCCP. See section 2.3 of the Guideline for the Special Investigative Powers.
17 See subsection 2.2.2 under B.
18 See art. 126n DCCP.

This special investigative power thus refers to particular types of data that are specified in lower regulations. Traffic data in that list must be retained by public telecommunication service and network providers for law enforcement purposes.[19]

Traffic data that is available from online service providers can also be acquired using the special investigative power to obtain 'other data' from other persons, institutions, and companies. In this case, traffic data is considered as falling under the category of 'other data'. Art. 126nd(1) DCCP reads as follows:

(1) "In case of reasonable suspicion of a crime as defined in art. 67(1) DCCP and insofar it is in the interest of the investigation, a public prosecutor can issue a data production order to those who reasonably qualify as having access to certain stored or processed data"

The above-described detailed regulations in Dutch law show that data production orders for obtaining traffic data from online service providers are regulated in an accessible manner.

B Legislative history

Dutch legislative history specifies which legal basis is applicable for obtaining traffic data from electronic communication service providers and other persons, institutions, and companies.[20] However, it does not clarify on which legal basis data can be obtained from *online* service providers. This is in itself curious, given that in the recent past, the 'commission for data collection in the information society' was requested to determine which investigative powers for data collection were appropriate in our 'information society' (as the name of the commission suggests). The Dutch legislature deemed legislation related to collecting of information from persons, institutions, and companies of major importance in modern criminal investigations within our 'information society'. A former minister of justice stated that the 'digital revolution' required law enforcement authorities to have broad data collection powers.[21]

19 See 'Besluit vorderen gegevens telecommunicatie', *Stb.* 2006, 730.

20 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2001/02, 28 059, no. 3 (explanatory memorandum Act on Data Production Orders for Telecommunication Providers), p. 4-5. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum to the General Act on Data Production Orders), p. 13-14.

21 See Handelingen Eerste Kamer, 5 July 2005, 32-1498. In *Parliamentary Series II* 2003/04, 29 441, no. 6, p. 1 and p. 5. The legislature also referenced 'developments in information- and communications technology' that require a 'modernisation of criminal procedural law'.

Given the above, one would assume that the aforementioned special commission would spend ample time examining the regulations that are required to obtain data from all kinds of online service providers. Instead, the specially appointed commission and Dutch legislator primarily focused on the collection of data primarily available from telecommunication providers, banks, and travel companies located in the Netherlands.[22] The explanatory memoranda of the General Act on Data Production Orders and the Act on Data Production Orders for Telecommunication Providers did not even mention the importance of the availability of data at online service providers, other than internet access providers. Legislative history therefore does not shed light on the applicable regulations for online service providers (other than internet access providers). Of course, this finding may be explained by the fact that the advisory report was presented in 2001, when the consequences of digitalisation on both our society and criminal investigations could not yet be fully appreciated. The commission seemed well aware of this. In fact, it explicitly stated in its report that: *"The commission is aware that the development of our information society will continue and this will be of influence on our proposals. Our proposals are not the end of the road (…)."*[23] However, to date the report has been the end of the road with regard to creating legislation to obtain data from online service providers using data production orders.

C Case law

Case law that explicitly deals with the power to obtain traffic data from online service providers is scarce. In *one* case of the Court of Gelderland in 2013, the judgement details that traffic data had been obtained from online service providers to determine the identify of a suspect.[24] The judgment describes how internet traffic data relating to a specific e-mail account had been obtained by law enforcement officials. The traffic data consisted of logging data in the form of IP addresses that were generated after a user registered for service from a webmail provider. To obtain the IP addresses, law enforcement officials must have used the special investigative power to obtain either (1) traffic data (based on art. 126n DCCP) or (2) other data from electronic communication service providers (based on art. 126ng(1) DCCP jo art. 126nd DCCP). The case itself does not specify the legal basis that was used. No other case law that specifically indicates the legal basis for obtaining internet traffic data using a data production order issued to an online service provider is available.

22 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum to the General Act on Data Production Orders), p. 8 and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2001/02, 28 059, no. 3 (explanatory memorandum to Act on Data Production Orders for Telecommunication Providers), p. 4-6. See also the report by the Commission Mevis 2001, p. 20.

23 Translated from the report of the Commission Mevis 2001, p. 17.

24 See Rb. Gelderland, 23 April 2013, ECLI:NL:RBGEL:2013:BZ8768.

The scarcity of case law and the ambiguity regarding the applicable legal basis in the examined case illustrate the difficulty of determining exactly which regulations apply for this type of data production order that can be issued to online service providers.

D Public guidelines

The Guideline for Special Investigative Powers separates the legal regimes for data production orders that are issued to (1) (tele)communication service providers and (2) other persons, institutions, and companies.

The guideline indicates that, insofar as subscriber and traffic data cannot be acquired using the special investigative powers to obtain data from electronic communication service providers, the special investigative powers to obtain data from any other person, company, or institution can be used.[25] The guideline thus indicates a legal basis for the investigative method, although it is does not relate specifically to the issuing of data production orders regarding traffic data to online service providers.

6.1.3 Other data

The category of other data includes data that is not subscriber data, traffic data, or content data. For example, it may consist of individuals' profile information, which is available from social media providers. Profile information can help law enforcement officials to gather more information about an individual's background and network.[26]

The accessibility of the legal basis for obtaining other data is examined below using the announced research scheme.

A Statutory law

Other data can be acquired from online service providers using the special investigative power to obtain other data from those persons, institutions, and companies that have access to relevant stored data on the basis of art. 126nd DCCP.[27] The text of art. 126nd DCCP was detailed in subsection 6.1.2. There is no specific data production order to acquire other data from electronic communication service providers. Law enforcement officials must apply the special investigative power in art. 126nd DCCP to obtain this category of data. This is regulated in art. 126ng(1) DCCP. The text of art. 126ng(1) DCCP reads as follows:

25 Guideline for special investigative powers of 2014, p. 6. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum to the General Act on Data Production Orders), p. 13-14.

26 See subsection 2.2.2 under B.

27 See 126nd DCCP.

"(1) *"A data production order as meant in article 126nc, first paragraph, 126nd, first paragraph, or 126ne, first and third paragraph, and art. 126nf, first paragraph, can be issued to a provider of a communication service within the meaning of article 126la, insofar the data production order does not relate to data that can be obtained by applying articles 126n and 126na. (…)"*

The provision essentially states that data, which is not considered subscriber or traffic data, can be obtained with data production orders that are regulated as special investigative powers that can be issued to all other persons, institutions, or companies.

Under Dutch law, a separate special investigative power (art. 126nf DCCP) is applicable that regulates data production orders to obtain 'sensitive data'. In this study, it is taken as a point of departure that the category of other data can also encompass sensitive data. Profile information of an individual that is available at online services may be considered sensitive data.[28] As such, this special investigative power to obtain sensitive data in art. 126nf DCCP is also relevant in this context. Art. 126nf(1) DCCP reads as follows:

"In case of reasonable suspicion of a crime as defined in art. 67 DCCP, first paragraph, which, considering its nature and cohesion with other crimes the suspect committed seriously interfere with the legal order, a public prosecutor can, insofar the interest of investigation demands it, gain access to data as meant in art. 126nd(2) DCCP by use of data production orders"

The special investigative power in art. 126nf DCCP refers to art. 126nd(2) DCCP, in which the definition of sensitive data is provided. Art. 126nd(2) DCCP reads as follows.

(2) "The data production order referred to in the first paragraph cannot be issued to the suspect. Article 96a, third paragraph, shall apply mutatis mutandis. The data production order cannot relate to personal with regard to person's religion or belief, race, political opinions, health, sexual life or union membership"

The above-described detailed regulations in Dutch law show that data production orders for obtaining other data from online service providers are regulated in an accessible manner.

B Legislative history

The category of other data that can be obtained using data production orders was implemented in criminal procedural law after the General Act on Data Production Orders was ratified in 2005. The explanatory memorandum to that act explains that the category of sensitive data was adopted from data protection legislation.[29]

28 See further subsection 6.2.3.

29 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 10.

The collection of other data is privacy sensitive, particularly when the data falls under the category of sensitive data, and merits its own data production order with strong procedural safeguards, according to the Dutch legislator. The conditions to obtain sensitive data are examined in subsection 6.2.3.

C Case law

Case law regarding the application of the special investigative power to obtain other data from online service providers is scarce. There is only *one* case available that indicates the legal basis for obtaining other data from online service providers.[30] This case concerned bank fraud and money laundering offences committed by a criminal organisation. Data regarding irregular financial transactions and traffic data were both required to gather evidence for a bank fraud and money-laundering offence that was committed using online banking. The traffic data revealed an IP address that subsequently aided law enforcement officials in identifying a suspect. From the judgement in the case, it became clear that the investigative power to obtain other information in art. 126nd DCCP was used to acquire (1) all available information relating to an individual who held an account with an online access provider and (2) transactional data from (online) financial service providers.[31]

This judgement thus indicates that the special investigative power to obtain other data can be applied to online service providers in order to acquire all data associated with a user of a particular service based on art. 126nd DCCP (with the exception of sensitive data).

D Public guidelines

As explained in subsection 6.1.1, the Guideline for Special Investigative Powers of the Public Prosecution Service focuses heavily on gathering data from telecommunication service providers. It does not contain any specific sections concerning data production orders to gather other data and sensitive data. It also does not explicitly indicate which legal basis in Dutch criminal procedural law is used to obtain other (sensitive) data from online service providers.

6.1.4 Content data

The category of content data includes data that relates to the meaning or message conveyed through a communication. This category of data consists of private messages that can be sent using electronic communication service providers and online service providers. Arguably, it also entails stored documents that are available from these providers. Law enforcement officials

30 See Rb. Noord-Holland, 27 October 2014, ECLI:NL:RBNHO:2014:10014.
31 See Rb. Noord-Holland, 27 October 2014, ECLI:NL:RBNHO:2014:10014.

can use this data to learn about a suspect and his surroundings, which can influence their use of other investigative methods (see Odinot et al. 2012, p. 91-94).[32]

The accessibility of the legal basis for obtaining content data is examined using the announced research scheme.

A Statutory law

Data that is stored at electronic communication service providers can be obtained with a specific data production order that is regulated as a special investigative power in art. 126ng(2) of the DCCP.[33] The provision refers back to art. 126ng(1) DCCP. Therefore, the first two sections of art. 126ng DCCP are provided below.

(1) *"A data production order as meant in article 126nc, first paragraph, 126nd, first paragraph, or 126ne, first and third paragraph, and art. 126nf, first paragraph, can be issued to a provider of a communication service within the meaning of article 126la, insofar the data production order does not relate to data that can be obtained by applying articles 126n and 126na. The data production order cannot relate to data that is stored on an automated device of the provider, which is not intended or originated from him."*

(2) *"In case of reasonable suspicion of a crime as defined in art. 67 DCCP, first paragraph, which, considering its nature and cohesion with other crimes the suspect committed seriously interferes with the legal order, a public prosecutor can, insofar the interest of investigation demands it, issue a data production order to those who reasonably qualify as having access to data as meant in the last sentence of section one, to collect data where they evidently originate from the suspect, are intended for him or relate at him, or have served to commit the offense, or when the offense was apparently committed in relation to that data."*

The above provision is formulated in a complex manner. In brief, it states that stored at an electronic communication service provider that cannot be obtained with any of the other data production order that is issued to a person, institution, or company, can be obtained under stringent conditions, including a warrant of an investigative judge (see art. 126ng(4) DCCP). As is shown below, other legal sources state that stored e-mails can be obtained at electronic communication providers under this provision. Keeping mind that content data is a category of data that relates to the meaning or message conveyed through a communication, it should be concluded that art. 126ng(2) DCCP provides an indication of the applicable legal basis for the investigative method.

32 See subsection 2.2.2 under B.
33 Art. 126ng(2) DCCP.

B Legislative history

The explanatory memorandum to the General Act on Data Production Orders explains art. 126ng(2) DCCP is specially designed to obtain "*the contents of an e-mail that is stored at an internet provider*".[34] The provision finds its background in the right to private correspondence. Legislative history thus provides an indication of the provision that is applicable to obtain content data, restricted to stored e-mails, from online service providers.

C Case law

Currently only *one* case that explicitly refers to the appropriate legal basis for obtaining content data from online service providers is available. The case, which has already been discussed in subsections 2.5.4, concerns a drug investigation in which law enforcement officials wanted to obtain access to messages in a webmail account to determine where a shipment of cocaine was going to be delivered. To pursue that goal and obtain the desired data, law enforcement officials obtained remote access to the account and conducted a search.

In first instance, the Court of Rotterdam decided that access to the webmail account's contents should have been obtained using the special investigative power as regulated in art. 126ng(2) DCCP.[35] The court's judges described how the data production order should have been sent to the Microsoft Corporation, which provides the webmail service Hotmail (now Outlook), with an accompanying mutual legal assistance request to the U.S. Department of Justice.

This judgement thus indicates that the special investigative power in art. 126ng(2) DCCP is the appropriate legal basis for issuing a data production order to obtain content data in the form of stored e-mails from online service providers.

D Public guidelines

The Guideline for Special Investigative Powers repeats legislative history. It states that stored e-mails available at electronic communication service providers should be obtained using the special investigative power provided in art. 126ng(2) DCCP.[36] The guideline does not further elaborate on the appropriate legal basis for obtaining other information that may be regarded as content data that may be available at (other) online service providers.

34 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 14 and 26.

35 Rb. Rotterdam, 26 April 2010, ECLI:NL:RBROT:2010:BM2519.

36 See section 2.3 and 2.4 of the guideline.

6.1.5 Section conclusion

The legal basis in Dutch law for data production orders that are sent to online service providers are considered to be *accessible*. Data production orders with regard to the types of data distinguished generally are regulated in detail as special investigative powers in the DCCP. This statutory law and the other examined sources in the law together provide an indication of the applicable legal basis in Dutch law for the identified types of data production orders that can be issued to online service providers. Yet, a degree of ambiguity is present about the applicable legal basis for data production orders that are sent to online service providers, due to the dual regime for data production orders for (1) electronic communication service providers and (2) all other persons, institutions, or companies. It is not clear for all online service providers whether they are considered as an electronic communication service provider.

6.2 Foreseeability

A foreseeable legal framework is a legal framework that prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which the investigative method is exercised.[37]

The ambiguity that is created by the dual regime for data production orders also affects the foreseeability of the regulations of data production orders. It is unclear exactly which online service providers are regarded as electronic communication service providers. It is therefore not always clear whether a data production order should be issued that is designed for an electronic communication service provider or for all other persons, institutions, or companies. This ambiguity especially influences clarity about the manner the investigative method is applied in practice.

The foreseeability of the Dutch legal basis for data production orders with regard to all four types of data (i.e., subscriber data, traffic data, other data, and content data) is further examined in subsections 6.2.1 to 6.2.4. Subsection 6.2.5 then presents conclusions regarding the foreseeability of the Dutch legal framework for each the data production orders explored.

37 See subsection 3.2.2 under B.

6.2.1 Subscriber data

The foreseeability of the legal basis for obtaining subscriber data is examined below using the announced research scheme.

A Statutory law

The special investigative power that can be applied to obtain subscriber data from electronic communication service providers indicates the scope of investigative power and describes the conditions under which subscriber data can be obtained. Art. 126na DCCP lists that law enforcement officials can obtain the following data: (1) name, (2) address, (3) postal code, (4) city, (5) number, and (6) type of service used by the subscriber.[38] A law enforcement official can order the production of subscriber data in criminal investigations with regard to all crimes.

The special investigative power to obtain subscriber data from any person, institution, or company also details the scope of the investigative power and the conditions under which the special investigative power can be exercised. Art. 126nc DCCP specifies that the following data can be obtained with a data production order: (a) name, address, city, and postal address; (b) date of birth and gender; (c) administrative data; and (d) type of business and location of its headquarters (if the data is obtained from a company).[39] Law enforcement officials can also apply this special investigative power in criminal investigations with regard to any crime.

The detailed provisions for the investigative powers with detailed lists of subscriber data clearly indicate the scope of the investigative method and the manner in which the investigative methods are exercised.

B Legislative history

Dutch legislative history explains that e-mail addresses and IP addresses are considered to be part of the 'numbers' category in the special investigative power to obtain subscriber data in art. 126na DCCP.[40]

Dutch legislative history also explains that the (sub)category of 'administrative data' in the special investigative power for subscriber data in art. 126nc DCCP is considered to be 'registration information' about an individual that may be available at the person, institution, or company.[41] Registration information may consist of a user account number or a bank account number that is associated with an individual.[42]

---

38 See art. 126na DCCP.

39 See art. 126nc DCCP.

40 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2001/02, 28 059, no. 3 (explanatory memorandum Act on Data Production Orders for Telecommunication Providers), p. 11.

41 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 21.

42 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 21.

C Case law

As explained in subsection 6.1.1, an IP address that is registered by an online service provider is considered subscriber data. Case law shows that this data can be acquired using the special investigative power to obtain subscriber data from electronic communication service providers in art. 126na DCCP.[43]

D Public guidelines

The Guideline for Special Investigative Powers specifies the manner in which subscriber data can be obtained from (tele)communication service providers.[44] However, it does not provide further information regarding the scope of the investigative method. This is also not necessary, given the detailed regulations that exist in statutory law and legislative history.

6.2.2 Traffic data

The foreseeability of the legal basis for obtaining traffic data is examined below using the announced research scheme.

A Statutory law

The legal basis in Dutch criminal procedural to obtain traffic data from online service providers does not indicate the scope of the investigative method. As explained in subsection 6.1.2, the two special investigative powers (art. 126n DCCP and art. 126nd DCCP) regulate data production orders concerning traffic data. Both state that public prosecutors can order the production of the data in identical conditions. In criminal investigations, prosecutors can order the mandatory production of traffic data with regard to crimes as defined in art. 67(1) DCCP. The collection of data must be of interest to the investigation.[45] Crimes as defined in art. 67 DCCP are crimes that are considered more severe than others and allow for custodial prison sentences.[46] Cybercrimes fall into this category of crime.[47]

The *scope* of the investigative power to obtain traffic data can be derived from telecommunication law. Article 2 of the 'Regulation to Obtain Telecommunications Data' specifies that the following categories of data can be obtained under this special investigative power:

---

43 See, e.g., Rb. Amsterdam, 1 October 2009, ECLI:NL:RBAMS:2009:BK1564, Rb. Groningen, 20 May 2010, ECLI:NL:RBGRO:2010:BM5193, and Rb. Overijssel, 9 April 2013, ECLI:NL:RBOVE:2013:BZ6638.

44 For instance, the guideline explains how Dutch law enforcement authorities use the 'CIOT system' to obtain subscriber and traffic data from public telecommunication service providers. CIOT stands for "Centraal informatiepunt onderzoek telecommunicatie". See for more information about the workings of the system, see: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2010/07/01/factsheet-ciot/informatieblad-ciot.pdf (last visited on 22 March 2015).

45 See art. 126n DCCP and art. 126nd DCCP.

46 As specified in art. 67(1)(a) DCCP.

47 As specified in art. 67(1)(b) DCCP.

(1) Name, address, and city of the subscriber;
(2) Numbers of the subscriber;
(3) Name, address, city and number of the person connected to the subscriber;
(4) Date and time that a connection started and ended;
(5) Location data for the network connecting devices;
(6) The numbers and types of devices used by the subscriber;
(7) The types of services used by the subscriber; and
(8) The name, address, and residence of the person who pays the bill.[48]

It is important to emphasise that the above regulations for telecommunication providers only apply to *public telecommunication network providers* and *public telecommunication service providers*.[49] Legislative history indicates that certain online service providers – such as (a) webmail providers, (b) communication service providers that make use of apps to facilitate communications, and (c) social media providers – do not fall into these categories of public telecommunication providers (cf. Odinot et al. 2013, p. 102-103 and p. 106).[50] Online storage providers are also likely not included to these categories.

Smits (2006, p. 77) provides a clear distinction between public telecommunication providers and online service providers, stating that public telecommunication service providers mainly consist of network and service providers that are able to influence the transport (i.e., routing) of telephone or internet traffic. Online service providers that match that description are typically *internet access providers*.

Nevertheless, even when the online service provider involved is not regarded as a public telecommunication network or service provider, law enforcement officials can obtain traffic data from persons, institutions, and companies (including online service providers) using the special investigative power to obtain other data.[51] This entire issue illustrates just how complex the Dutch legal framework for data production currently is.

48 See also art. 5 of the data retention directive (2006/24/EC) and the appendix of the Dutch Telecommunications Act to art. 13.2a. These regulations specify the same list of data that can be obtained with the special investigative power in art. 126n DCCP.

49 See art. 13.2a(2) Dutch Telecommunications Act.

50 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2007/08, 31 145, no. 9, p. 6 and *Kamerstukken I* (Parliamentary Proceedings First Chamber) 2008/09, 31 145, no. F, p. 4 and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 537, no. 3 (explanatory memorandum amended Data Retention Act), p. 43. See also Opinion 02/2013 on apps on smart devices, art. 29 Data Protection Working Party, 00461/13/EN WP 202, p. 25, note 46.

51 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 13-14.

B Legislative history

Dutch legislative history states that traffic data relates to the *external characteristics* of network traffic and not its contents.[52] This statement leaves substantial room for interpretation with regard to the question of what traffic data actually comprises. For example, it remains unclear whether (a) data with regard to search terms, (b) links to websites, (c) domain names, and (d) subject lines in private messages must be considered as content or traffic data (see Koops & Smits 2014, p. 93-106).[53] The analysis of statutory law under A above has shown that telecommunication service providers do not retain this information as traffic data for law enforcement purposes. However, it is unclear whether this kind of information is retained by telecommunication providers and other providers for different purposes and whether that information can be obtained with other data production orders.

Law enforcement officials can acquire 'other traffic data' by using the special investigative power to obtain 'other data' from all persons, institutions, and companies. Dutch legislative history explains that the other data category consists of a broader range of data than described in telecommunications law.[54] The legislator discusses this category as data concerning information regarding the services that are provided to a subscriber, such as the duration of a service and other subscriber-related data.[55] This includes bank account and billing information (cf. Spapens, Siesling & de Feijter 2011, p. 26).[56] From this description in legislative history, it follows that logging data about a user of an online service can be obtained using this special investigative power. In other words, the category of other data is considerably broader than traffic data (although sensitive data is explicitly excluded from the special investigative power).

C Case law

Case law that deals with the legal basis for obtaining traffic data from online service providers is scarce in the Netherlands. However, *one* relevant case is available that illustrates the scope of the investigative method.[57] The case involved law enforcement officials attempting to identify an individual who

52 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2001/02, 28 059, no. 3 (explanatory memorandum Act on Data Production Orders for Telecommunication Providers), p. 7.

53 With reference to Asscher & Ekker 2003, p. 104, Koops 2003, p. 77-78, Smits 2006, p. 416, Steenbruggen 2009, p. 56.

54 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 8.

55 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 8.

56 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 8.

57 See Rb. Noord-Holland, 11 February 2016, ECLI:NL:RBNHO:2016:1023. See also RTV Noord-Holland, 'IJmuidense V&D-dreiger was werknemer V&D', 28 October 2015. Available at: http://www.rtvnh.nl/nieuws/173286/live-ijmuidense-vd-dreiger-vandaag-voor-de-rechter (last visited on 3 March 2016).

had threatened to bomb a retail shop in the Netherlands. The case is highly interesting, as the suspect made the threats using online services and tried to hide his originating (public) IP address. Although no details about the applicable legal basis of the data production orders are provided in the judgment, it can be derived from the case details that to identify the suspect, internet traffic data was obtained from (1) internet access providers, (2) e-mail services, and (3) the micro blog service Twitter. The case is further considered below to illustrate both the scope of the investigative power and how the investigative power is applied in practice.

The CricusBloed bomb threat investigation
The facts of the case are as follows. The suspect first registered an e-mail account at the '10 Minute Mail' webmail service. Next, he created an online Twitter account under the name of 'CricusBloed'. Using his mobile phone, he then published bomb threats to Twitter that were directed to a Dutch warehouse store.

Following the bomb threats, Dutch law enforcement officials issued an emergency request to Twitter to disclose traffic data relating to the relevant Twitter account. Twitter responded by disclosing the following information (translated from Dutch in the court judgement):

the account 'CricusBloed' was created on 24 September 2013 at 20:00:25 hours with the e-mail address [fakemail address].

An individual logged in to Twitter several times on Twitter. These are as follows:
2013-09-25 02:20:30, last_login_ip: [IP address 2]
2013-09-25 02:19:00, last_login_ip: [IP address 2]
2013-09-24 20:25:55, last_login_ip: [IP address 3]
2013-09-24 20:25:40, last_login_ip: [IP address 3]
2013-09-24 20:19:58, last_login_ip: [IP address 4]
2013-09-24 20:13:57, last_login_ip: [IP address 4]
2013-09-24 20:13:32, last_login_ip: [IP address 5]
2013-09-24 20:09:29, last_login_ip: [IP address 6]
2013-09-24 20:06:31, last_login_ip: [IP address 1]
2013-09-24 20:04:51, last_login_ip: [IP address 1]

Research indicated the IP addresses belong to:
[IP address 2] Vodafone Mobile Office Nederland
[IP address 3] SpaceDump IT, Tor exit node, location Sweden
[IP address 4] Nforce Entertainment, Tor exit node network, location the Netherlands
[IP address 5], Kaia Global Networks, Tor exit router, location Germany
[IP address 6], BROADNET, possibly Tor exit node, location Norway
[IP address 1], Chaos Computer Club, possibly Tor exit node, location Germany

As can be seen from the above list of traffic data, only the Vodafone IP address does not belong to a Tor exit relay.[58] This provided the lead that Dutch law enforcement officials needed to track the suspect down. However, the suspect made use of his mobile phone to issue the bomb threats via Twitter. At that specific moment in time, approximately 60,000 mobile phones in the Netherlands were connected to the Internet via Vodafone using the same IP address. Vodafone thus apparently did not have the means to identify a specific user.[59]

In their quest to identify the suspect, law enforcement officials next requested, likely using the special investigative power to obtain subscriber data from electronic communication service providers in Dutch law, to obtain subscriber data from 10 Minute Mail. This online service provider disclosed an IP address that was registered when the webmail account was created. It was then determined that this IP address was allocated by Ziggo, a Dutch internet access provider. Once law enforcement officers were able to obtain subscriber data from Ziggo, they had the lead they needed to track the suspect's home address down.

After law enforcement officials searched the suspect's residence, the digital forensics analysis of the contents stored on his laptop, mobile phone, and internet router provided them with further evidence that the suspect had posted the bomb threats on Twitter from his home address.[60] Furthermore, the location (i.e., traffic) data of the suspect, which was (eventually) disclosed by his mobile phone provider, provided law enforcement officials with further evidence that positioned the suspect at his home address at the time of the bomb threats. The Court of Noord-Holland subsequently sentenced the suspect to 240 hours of community service for making the bomb threats.

D Public guidelines

The Dutch Radiocommunications Agency's guideline concerning data retention specifies which data is considered traffic data and can be obtained by the special investigative power as regulated in art. 126n DCCP.[61] However, it does not provide new information to the telecommunication regulations (examined under A above), since the both lists specify the same information.

58 A Tor exit relay is the last server from which the Tor network traffic exists. See subsection 2.3.2 for further explanation about the workings of the Tor system.

59 For more on this problem, see Kerkhofs and Van Linthout 2013, p. 205-207. The new Data Retention Act seeks to solve the problem by requiring the retention of more data. See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 537, no. 3 (explanatory memorandum amended Data Retention Act), p. 41-42.

60 For instance, the data on his laptop showed how the suspect searched for '10 Minute Mail' during the same period as the bomb threats and activity on Twitter on his mobile phone took place at the same time of the posted bomb threats.

61 The guideline is available at http://www.rijksoverheid.nl/documenten-en-publicaties/richtlijnen/2010/12/21/toelichting-bewaring-gegevens-Internet.html (last visited on 8 November 2015).

6.2.3 Other data

The foreseeability of the legal basis for obtaining other data is examined using the announced research scheme.

A Statutory law

Data production orders for online service providers can be used to acquire other data when law enforcement officials utilise the special investigative power to obtain other data from persons, institution, or companies.[62] No specific data production order is created to obtain other data from electronic communication service providers. Therefore, the special investigative power that can be directed to all persons, institution, or companies must be used.[63]

The special investigative power itself specifies that a public prosecutor can order the mandatory production of traffic data in criminal investigations with regard to crimes as defined in art. 67(1) DCCP (including cybercrimes). The collection of data must be in the interest of the investigation.[64] Statutory law thus clarifies how the investigative method is applied in practice.

However, the *scope of the investigative method* remains unclear. The reason is that the other data category is particularly broad in its wording. The special investigative power does stipulate that sensitive data, i.e., personal data relating to an individual's religious beliefs, race, political affiliations, health, sexual life, and union membership, can only be obtained using a different special investigative power.[65] However, this leaves a broad category of data in between that may be considered as other data.

Sensitive information can only be obtained by law enforcement officials using the special investigative power in art. 126nf DCCP that can only be applied under stringent conditions. These conditions are as follows: (1) authorisation must be granted by a public prosecutor, (2) a warrant must be issued by an investigative judge, and (3) the data production order may only be used in criminal investigations of crimes as defined in art. 67(1)

62 See art. 126nd DCCP.

63 See art. 126ng(1) DCCP jo art. 126nd DCCP.

64 See art. 126nd DCCP. A warrant of an investigative judge is required to obtain other data using the data production orders in criminal investigations relating to other crimes (see art. 126nd(6) DCCP.

65 See art. 126nd(2) DCCP. The other special investigative power is specified in art. 126nf DCCP.

DCCP that (4) seriously infringe the legal order[66], and (5) the collection of the relevant data must be essential to furthering the investigation.[67]

B Legislative history

Dutch legislative history explains that the special investigative power to obtain other data concerns a broad category of data that may include data relating to services that are provided to a subscriber.[68] As explained in subsection 6.2.2, the data may include information about a subscriber's user account, bank account, and billing arrangements.

Dutch legislative history also explains that the type of data that is considered to be sensitive data, is derived from data protection regulations.[69] More stringent legal thresholds apply when law enforcement officials wish to obtain sensitive data.[70]

C Case law

The Dutch Supreme Court has clarified that photographs of a person (taken for a public transportation chip card) that are obtained with data production orders that are issued to public transportation companies are considered sensitive data. However, (lower) Dutch courts decided that photographs that are taken of individuals by banks (in the form of footage from both automated teller machine and CCTV surveillance cameras) in public places are not considered 'sensitive data' (cf. Zwenne & Mommers 2010, p. 238-

66 Whether crimes 'seriously infringe the legal order' depends on the circumstances of a case (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 24. See further Blom 2007. The question if cybercrimes, such as hacking and the distribution of malware, are crimes that seriously infringe the legal order will depend on the consequences, in both economic terms and the consequences of the crime for the victims. The Dutch legislator seeks to amend the legal thresholds for special investigative powers within Dutch criminal procedural law. Their intention is to replace the more abstract criteria of a 'serious interference with the legal order' and 'essential to furthering the investigation' with criminal investigations that refer to the maximum sentences of crimes. The proportionality test and subsidiarity test that apply to all special investigative powers will then be codified in the introduction to the provisions in criminal procedural law for pre-trial investigations (see the discussion document regarding the general provisions for pre-trial investigations, p. 24 (6 June 2014).The question that arises is whether a meaningful proportionality test and subsidiarity test is still conducted when these criteria are erased from the special investigative powers. See further Ölçer 2015, p. 304 and Van Buiten 2016. This discussion is not further addressed in this study.

67 This requirement serves to emphasise that a test is conducted to determine whether the collection of data is proportionate and no less privacy infringing investigative powers are available, considering the circumstances at hand (cf. Franken 2009, p. 83).

68 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 8.

69 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 10 referring to art. 16 and 18 of the Dutch Data Protection Act.

70 See subsection 6.1.3.

239.)[71] This raises the question whether profile information from online service providers, that often include photographs, can only be obtained using the special investigative power to obtain sensitive data in art. 126nf DCCP or also with the special investigative power to obtain other data in art. 126nd DCCP.

The Dutch legislator has also explained in legislative history that photographs of individuals are to be considered sensitive data.[72] The Dutch legislator has further stated in the explanatory memorandum of the General Act on Data Production Orders that the special investigative power to obtain sensitive data is only appropriate when it is clear *upfront* that the requested data concerns 'sensitive data'.[73]

It is common knowledge that user profiles from social media providers often contain (a) one or more photographs of the user, (b) the user's political views, and (c) information with regard to the user's sexual orientation. It therefore seems apparent that law enforcement officials should use the special investigative power to obtain sensitive data when they seek to obtain profile information from a social media service. Due to a lack of case law, it is not clear which special investigative power is used in practice to acquire profile information from online service providers.

D Public guidelines

The Guideline for Special Investigative Powers does not provide specific information regarding the application of the special investigative power to obtain other data from online service providers.[74]

6.2.4 Content data

The foreseeability of the legal basis for obtaining content data is examined below using the legal sources explored above.

A Statutory law

The DCCP requires the use of the special investigative power in art. 126ng(2) DCCP to obtain data stored in computers at electronic communication service providers.[75] Strict conditions must be met to use this special investigative power.[76] These conditions are as follows: (1) an order must be obtained

71 HR 23 March 2010, ECLI:NL:HR:2010:BK6331. See, e.g., Rb. Rotterdam, 19 May 2010, ECLI:NL:RBROT:2010:BM5003, Rb. Alkmaar, 5 August 2010, ECLI:NL:RBALK:2010:BN3312, Rb. Den Haag, 26 September 2011, ECLI:NL:RBSGR:2011:BU3207, and Rb. Amsterdam, 7 April 2015, ECLI:NL:RBAMS:2015:1987.

72 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1997/1998, 25 892, no. 3 (explanatory memorandum of the Data Protection Act), p. 105.

73 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 7.

74 See also subsection 6.1.3 under D.

75 Art. 126ng(2) DCCP. See also subsection 6.1.4.

76 See art. 126ng(2) DCCP.

from a public prosecutor, (2) a warrant must be issued by an investigative judge, (3) the data production order may only be used in criminal investigations of crimes as defined in art. 67(1) DCCP that (4) seriously infringe the legal order, and (5) the collection of the relevant data must be essential to furthering the investigation.

The scope of the investigative power itself is not further explained in statutory law, which leaves the question of what exactly is meant by 'data stored on computers from electronic communication service providers' open.

B Legislative history

The explanatory memorandum to the General Act on Data Production Orders clearly states that e-mails available at online service providers can only be obtained under the special investigative power as articulated in art. 126ng(2) DCCP. Stringent requirements apply to this special investigative power. These requirements also act as safeguards, which are deemed appropriate for e-mails that are protected under the right to respect for correspondence.[77]

However, legislative history does not provide other examples of data that is stored on computers from electronic communication services providers that can be obtained under the special investigative power (other than e-mail). Based on the rationale of providing e-mails with special protection (to respect the right to correspondence), it is likely that the special investigative power also applies to stored private messages that users sent from social media service providers. This is because both types of messages can be considered 'correspondence', which is a special object of protection under art. 8 ECHR. However, whether stored documents available at online (storage) providers must be obtained with the special investigative power in art. 126ng(2) DCCP remains ambiguous.[78]

Are stored documents other data or content data?

Dutch legislative history does not identify which special investigative power must be used to obtain *stored documents* that are available at online service providers. The question at issue in this regard is whether stored documents qualify as (stored) 'other data' as meant in art. 126nd DCCP or 'stored data available at electronic communication service providers' (qualifying as content data) as meant in art. 126ng(1) DCCP.

77 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 14. See also the report of the Commission Mevis of 2001, p. 89. Art. 13 of the Dutch Constitution specifically protects communications sent by letter (art. 13(1)), telephone or telegraph (art. 13(2)).

78 See also subsection 6.2.4.

As explained above, the special protection for e-mails stems from the right to respect for correspondence. Stored documents that are available at online service providers are not necessarily correspondence. Thus, one can argue that a public prosecutor can acquire stored documents using the special investigative power to obtain 'other data' (cf. Koops et al. 2012b, p. 43-44). As explained in subsection 6.1.2, most online service providers can be considered electronic communication service providers. Based on the wording of the special investigative power to obtain 'stored data that is available at electronic communication service providers' in art. 126ng(1) DCCP, it is in my view likely that this special investigative power to obtain content data is also applicable when law enforcement officials seek stored documents, because the investigative methods is particularly intrusive and the documents may contain correspondence.

C Case law

Only *one* case affirms that stored e-mails that are available at online service providers, more particularly webmail providers, should be obtained using the special investigative power as articulated in art. 126ng(2) DCCP.[79] The case, concerning the situation in which a law enforcement official was ordered by a public prosecutor to log in to a webmail account to learn the details about a shipment of cocaine to the Netherlands, is already extensively considered in subsection 6.1.4, it is not further discussed here.

D Public guidelines

The Guideline for Special Investigative Powers affirms that e-mail (and stored voice messages) can only be obtained from electronic communication service providers on the basis of art. 126ng(2) DCCP.[80] No further information is provided in this guideline regarding other data that can be obtained using this special investigative power.

6.2.5 Section conclusion

The results of the analyses conducted in subsections 6.2.1 to 6.2.4 with regard to the scope of the investigative methods are summarised in the Table 6.1.

79 Rb. Rotterdam, 26 March 2010, ECLI:NL:RBROT:2010:BM2520 and Hof Den Haag, 27 April 2011, ECLI:NL:GHSGR:2011:BR6836.

80 See sections 2.3 and 2.4 of the Guideline for Special Investigative Powers.

Applicable special investigative power	Scope of the investigative method
The special investigative power to obtain subscriber data from: A. electronic communication service providers (e.g., telecommunication service providers)	Category A: (1) name, (2) address, (3) postal code, (4) place of residence, (5) number, (6) type of service used by the subscriber.
B. other persons, institutions, and companies	Category B: (1) name, (2) address, (3) place of residence, (4) postal code, (5) data of birth, (6) gender, (7) administrative data, (8) type of business and location of headquarters.
The special investigative power to obtain traffic data from: A. electronic communication service providers (e.g., telecommunication service providers)	Category A: (1) name, address, and place residence of the subscriber, (2) numbers of the subscriber, (3) name, address, place residence and number of the person connected to the subscriber, (4) date and time that a connection started and ended, (5) location data for network connecting devices, (6) the numbers and type of devices used by the subscriber, (7) the types of services used by the subscriber, (8) name, address, and place of residence of the person that pays the bill.
B. other persons, institutions, and companies	Category B: all data regarding the services that are provided to a subscriber, such as information about the service provided and other data that is available about the subscriber of a service (incl. financial data, but not sensitive data).[81]
The special investigative power to obtain other data from every person, institution, or company (incl. electronic communication service providers)	All data regarding the services that are provided to a subscriber, such as the duration of the service and other subscriber-related data (incl. financial data, but not sensitive data).
The special investigative power to obtain content data from electronic communication service providers	E-mails and most likely private messages stored at electronic communication service providers.

Table 6.1: Overview of the applicable special investigative powers in the DCCP and the types of information that they may be used to obtain.

Table 6.1 shows that detailed regulations are available for data production orders in Dutch criminal procedural law. Nevertheless, the Dutch legal framework for data production orders *cannot be considered foreseeable* for data production orders that are issued to online service providers with regard to (1) subscriber data, (2) traffic data, (3) other data, and (4) content data.

81 Sensitive data is personal data relating to an individual's religious beliefs, race, political affiliations, health, sexual life, or union membership.

The dual regime for data production orders in Dutch criminal procedural law creates ambiguity with regard to which online service providers are considered (a) electronic communication service providers, (b) public telecommunication (service or network) providers, or (c) other persons, institutions, and companies. As a result, it is sometimes unclear which special investigative power must be used to acquire the identified categories of data from online service providers by issuing data production orders.

Furthermore, specific categories of data production orders are not regulated in a foreseeable manner in the Netherlands. The category of traffic data is not foreseeable, since the list of data only applies to data that is retained by public telecommunication (service or network) providers. It is also not clear whether stored documents should be placed within the category of other data or content data.

In other words, the Dutch legal regime for data production orders lacks clarity. A substantial lacuna exists in Dutch law concerning both the 'Who-question' (To whom can data production orders be issued and on which legal basis?) and the 'What-question' (What data can be obtained with the data production order regulated as a special investigative power in Dutch law?). These questions should be addressed in an amended legal regime for data production orders, which should preferably have only one tier of regulations.

6.3 Quality of the law

The normative requirement regarding the quality of the law, means that the ECtHR can specify the level of detail required for the description the investigative power and the minimum procedural safeguards that must be implemented vis-à-vis a particular method that interferes with the right to privacy. The detail that the ECtHR requires in the law and procedural safeguards depends on the gravity of the privacy interference that takes place.[82]

The desired quality of the law requirements in art. 8 ECHR for data production orders that are issued to online service providers was formulated in subsection 4.2.3 of chapter 4. The analysis showed that detailed regulations are desirable for the investigative method. In terms of the desired procedural safeguards, a distinction must be made for the different types of type of data, since issuing production orders for the different types interferes with the right to privacy in different ways. The desired quality of the law is visualised in the scale of gravity for privacy interferences regarding data production orders that are issued to online service providers in Figure 6.2.

82 See subsection 3.2.2 under C.

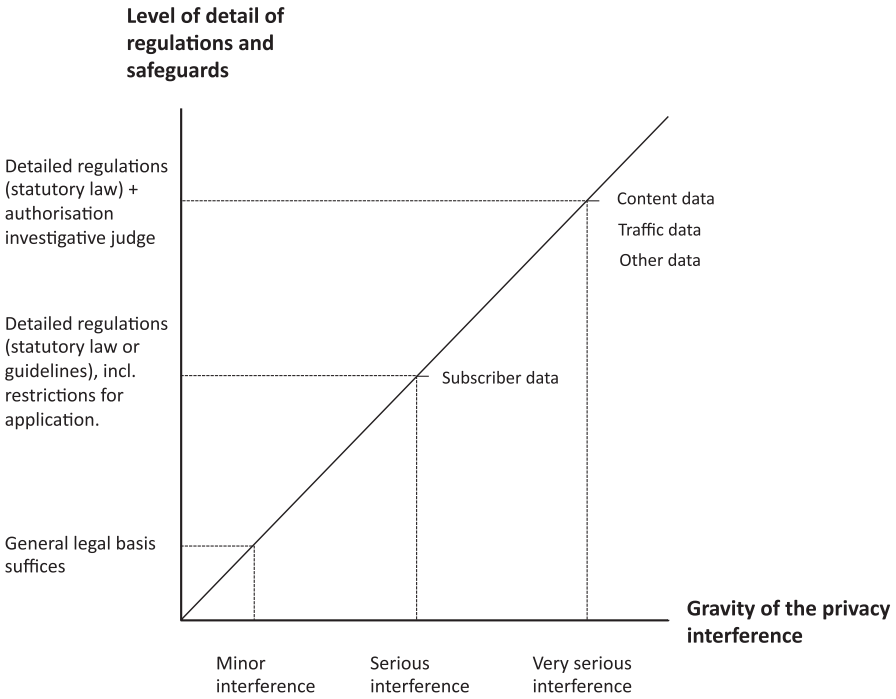

Figure 6.2: The scale of gravity for privacy interferences regarding data production orders that are issued to online service providers and the accompanying desired quality of the law.

The scale of gravity for privacy interferences in relation to data production orders and the accompanying desired quality of the law as depicted above in Figure 6.2 aid in determining whether the Dutch legal framework meets the desired quality of the law.

In subsections 6.3.1 to 6.3.4, the current quality of the law for all four types of data production orders is compared to the desired quality of the law. Subsection 6.3.5 presents conclusions regarding the quality of the Dutch legal basis for these digital investigative methods.

6.3.1 Subscriber data

The Dutch legal framework provides detailed regulations for obtaining subscriber data using a data production order.[83] The requirements (i.e., procedural safeguards) for issuing data production orders to acquire subscriber data are not stringent. As explained in subsection 6.2.1, law enforcement

83 Thereby, the Dutch legal framework also meets the positive obligation formulated in the case of *KU v. Finland* that forces contracting States to the ECHR to enable law enforcement authorities to obtain data from online service providers in order to identify internet users based on their IP address for the investigation of crimes.

officials can issue data production orders in criminal investigations related to any kind of crime.

Based on the minor intrusiveness of the privacy interference, no specific procedural safeguards were articulated as desirable procedural safeguards for the data production order in chapter 4. Therefore, the Dutch legal framework *meets the desired quality of the law* for the regulation of data production orders concerning subscriber data.

6.3.2 Traffic data

The special investigative power to collect traffic data from online service providers interferes with the right to privacy in a more serious manner than the special investigative power to obtain subscriber data. As defined in Dutch law, the traffic data category also concerns location data. The processing of location data is considered a privacy-intrusive investigative method, as law enforcement officials can obtain a detailed picture of certain aspects of an individual's private life by analysing the data. The analysis in subsection 6.2.2 has shown that public telecommunication (network or service) providers do not retain the destination IP address of network traffic under data retention legislation. Therefore, this sensitive data (which may indicate the website or web service an internet user visits) is therefore not especially stored for law enforcement purposes. However, the information may be retained nevertheless for other purposes and the information may be available at online service providers that are not telecommunication (network or service) providers.

Due to the more sensitive information that the traffic data category entails, the desirable quality of the law has been determined in chapter 4 as detailed regulations and mandatory authorisation from an investigative judge.[84] Several Dutch authors have argued that traffic data should only be collected under the same conditions as when stored correspondence is collected.[85] In the Netherlands, stored correspondence can only be obtained with a warrant from an investigative judge. The Dutch legislator acknowledges in legislative history that a serious privacy interference takes place when traffic and other data are collected from third parties.[86] More safeguards are therefore applicable to the collection of traffic data than to the collection of subscriber data. Traffic data may be collected when a *public prosecutor* orders a data production order in criminal investigations involving

84 See subsection 4.2.3.

85 See most notably Hofman 1995, p. 149 and 462, Dommering 2000, p. 72 and Asscher 2003, p. 24.

86 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2001/02, 28 059, no. 3 (explanatory memorandum Act on Data Production Orders for Telecommunication Providers), p. 4-5. *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory General Act on Data Production Orders), p. 10.

crimes stipulated in art. 67 DCCP. Therefore, the Dutch legal framework for obtaining traffic data currently *does not meet the desired quality of the law.*

The Dutch legislator considered raising the legal threshold for obtaining traffic data from electronic communication service providers by setting the requirement of a prior judicial warrant in 2015. This (concept) bill was the result of the annulment of data retention legislation. As discussed in subsection 5.3.2, the CJEU declared the data retention directive invalid in 2014. In 2015, the Court of The Hague also declared the Dutch data retention obligations invalid.[87] The data retention obligations were considered disproportionate in light of the rights to respect for private life and the protection of personal data.[88] In November 2015, the Minister of Security and Justice responded to the CJEU's judgement with a letter to the Dutch parliament and a new (concept) bill for data retention obligations.[89] In September 2016, an amended Data Retention Act was introduced to the Dutch Parliament.[90] The legislation aims to comply with the CJEU decision on data retention amending the investigative power for traffic data production orders by increasing the higher legal threshold of authorisation from a public prosecutor to a warrant from an investigative judge.[91] Under the new (amended) Data Retention Act, the proposed warrant requirement for the collection of traffic data meets the desirable quality of the law as identified in chapter 4.[92]

87 Rb. Den Haag, 11 March 2015, ECLI:NL:RBDHA:2015:2498.

88 Rb. Den Haag, 11 March 2015, ECLI:NL:RBDHA:2015:2498, par. 3.7.

89 See 'concept bill on data retention', p. 9 and 10 (available at: http://www.internetconsultatie.nl/dataretentie (last visited on 25 November 2015).

90 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 537, no. 2.

91 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 537, no. 3 (explanatory memorandum amended Data Retention Act), p. 2.

92 See also CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), para. 62: "*Above all, the access by the competent authorities to the data retained is not made dependent on a prior review carried out by a court of by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the object pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.*" Translating this decision to the Dutch legal framework, it is clear the CJEU prefers a prior warrant from an investigative judge to obtain traffic data that is retained as a consequence of a data retention measure. However, the problem remains that an interference takes place with the right to privacy of individuals by storing personal information about their communications that have nothing to do with serious crimes. See CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), para. 59. See also the report of the Raad van State, 17 July 2014, p. 11 and p. 16. Lastly, compare Diesfeldt and De Graaf (2015), who indicate the (2015) proposal for a data retention act meets the proportionality requirement, and Zwenne and Simons (2014), who are sceptical about the validity of the new data retention measure.

6.3.3 Other data

The application of the special investigative powers to obtain other data by law enforcement officials seriously interferes with the right to privacy. Law enforcement officials can obtain many different types of data from online service providers using several special investigative powers. Profile data that can be obtained from social media service providers can be particularly sensitive in nature. Law enforcement officials can also process and combine that data in order to acquire an intricate picture of certain aspects of individuals' private lives. In subsection 4.2.3, the desirable quality of law for this particular investigative method was articulated as detailed regulations with the procedural safeguard of a warrant from an investigative judge.

Dutch law currently *does not meet the desired quality of the law*, because it currently only requires authorisation from a public prosecutor. Considering the proposal of the Dutch legislator to require a warrant to obtain traffic (as described in subsection 6.2.3), it seems odd that a warrant requirement is not also being considered to regulate data production orders for obtaining other data. The privacy interference can be as serious in relation to both types of data production orders.

6.3.4 Content data

The special investigative power that enables law enforcement officials to obtain content data in the form of stored private messages from electronic communication service providers seriously interferes with involved individuals' right to respect for private life and correspondence.

Subsection 4.2.3 articulated the desired quality of the law for this investigative method, which encompasses detailed regulations for the investigative method with the procedural safeguard of a warrant requirement. In the Netherlands, it is clear that law enforcement officials must obtain a warrant to gather stored e-mails (and likely other stored private messages) located at online service providers. However, the detailed regulations do not further specify what other information is considered to be content data and hence is protected by these same strict requirements. The conclusion is therefore that the Dutch regulations for data production orders concerning content data do *not meet the desired quality of the law* where other data than stored e-mails and private messages are concerned. The analysis shows how the normative requirements of foreseeability and the quality of the law can be intertwined.[93] In relation to content data, the lack of foreseeability of the regulations related to the investigative methods influences the quality of the law.[94]

93 See also subsection 5.5.1.

94 However, the lack of the warrant requirement is most important.

With specific regard to stored documents that are available at online service providers, the procedural safeguard of a warrant is also considered to be desirable. When a warrant is required, an investigative judge can perform an additional proportionality test and determine whether it is appropriate to restrict the order to disclose the data. For instance, a data production order can be restricted to documents that fall within a certain time period or are selected after applying a (software) filter. As the analysis in subsection 6.2.4 has shown, it is unclear whether Dutch law currently requires authorisation (i.e., a warrant) from an investigative judge to obtain stored documents from online service providers. For that reason, the Dutch regulations to obtain content data using data production orders do *not meet the desired quality of the law*.

6.3.5 Section conclusion

The analyses in subsections 6.3.1 to 6.3.4 showed that the Dutch legal framework for the regulation of data production orders generally does not meet the desired quality of the law. Stronger procedural safeguards are suggested for data production orders with regard to traffic data, other data, and content data. In addition, the scope of the investigative methods must be established more clearly. Only the regulations concerning subscriber data production orders in Dutch law are deemed to be of sufficient quality.

6.4 Improving the legal framework

This section discusses how Dutch criminal procedural law can be improved to provide an adequate legal framework for data production orders that are issued to online service providers. A legal framework is considered adequate when (1) it is accessible, (2) it is foreseeable, and (3) the desired quality of the law is met. Table 6.2 summarises the results of the analyses concerning these normative requirements in sections 6.1 to 6.3.

Normative requirement	**Subscriber data**	**Traffic data**	**Other data**	**Content data**
Accessible	✓	✓	✓	✓
Foreseeable	✗	✗	✗	✗
Meets the desirable quality of the law	✓	✗	✗	✗

Table 6.2: Overview of the research results in sections 6.1 to 6.3 (✓ = adequate, ✗ = not adequate).

The suggested improvements to the Dutch legal framework for the regulation of data production orders that are issued to online service providers are based on these research results. A general improvement to the legal framework regulating data production orders is first proposed in subsection 6.4.1.

The specific improvements with regard to the Dutch legal framework are then proposed for each of the four types of data production orders (i.e., subscriber data, traffic data, other data, and content data) in subsections 6.4.2 to 6.4.5.

6.4.1 General improvement to the legal framework

A major improvement to the Dutch legal framework can be made by creating a single regime for data production orders in Dutch criminal procedural law (*Recommendation 1*). The current dual regime for data production orders is unnecessarily complex and therewith makes the framework less foreseeable to the individuals involved.[95] The Dutch legal framework with regard to data production orders can be made more straightforward by removing the dual regime for data production orders. Koops (2003, p. 119-120) already argued in 2003 that the division is unnecessary, since the same conditions apply to the special investigative powers for using data production orders to obtain almost all categories of data.

In a 2014 discussion document for reforming Dutch criminal procedural law, the Dutch Ministry of Security and Justice also stated that the dual regime for data production orders is redundant and proposed instead to create a single regime.[96] The greatest advantage of a single regime for data production orders in Dutch criminal procedural law is that it would remove some of the current complexity in the Dutch legal framework for data production orders. A second advantage is that the ambiguity that now exists with regard to which particular companies are considered 'electronic communication service providers' would disappear. Of course, as a prerequisite, the categories of data must be specified in lists in order to provide clarity regarding the scope of the special investigative powers regulating the data production orders.

6.4.2 Subscriber data

The DCCP provides a detailed legal basis for the issuing of using data production orders to obtain subscriber data. The special investigative powers in articles 126na DCCP and art. 126nc DCCP specify under which conditions the investigative method can be applied. In addition, a limited list of data indicates the scope of the investigative powers. I have argued that no further specific procedural safeguards are desirable for the regulation of this investigative method. Therefore, apart from creating a single legal regime to

95 See also subsections 6.2.4 and 6.2.5.

96 See the discussion document regarding special investigative powers (6 June 2014), p. 40-41. See also the letter of 30 September 2015 regarding the modernisation of the DCCP, p. 84. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (last visited on 3 October 2015). However, at the same time, the Dutch legislator proposed a new (concept) bill that amends data production orders concerning traffic data in November 2015 (see subsection 6.3.2).

obtain subscriber data, no further improvements to the Dutch legal framework for regulating data production orders concerning subscriber data are recommended.

6.4.3 Traffic data

The manner in which law enforcement officials can obtain traffic data using data production orders is regulated in an accessible manner in the Netherlands. However, the *scope* of the investigative powers to obtain traffic data is not sufficiently foreseeable to the individuals involved, due to the distinction between special investigative powers that apply to (1) public telecommunication network and service providers and (2) electronic communication service providers and (3) other people, institutions, or companies.

The foreseeability of the legal framework can be improved by stipulating in regulations outside of criminal procedural law what kind of data is considered traffic data. This type data can then be obtained from all people, institutions or companies under a single investigative power. Based on existing telecommunication regulations and the definition used in art. 1(d) of the Convention on Cybercrime, traffic data can be restricted to the following kinds of data: (1) the time, date, size, and duration of (a) network traffic or (b) calls to and calls from a subscriber; (2) the type of underlying service; (3) unique user ID(s) allocated to an individual; (4) the (dynamic) IP address allocated to a subscriber at the time of the communication; and (5) location data. Law enforcement officials can then obtain this data when they issue data production orders to online service providers, insofar as the service provider retains this information.[97]

In the 2016 proposal for an amended data retention act, the Dutch Minister of Security and Justice proposed a warrant requirement for collecting (internet) traffic data from public telecommunication providers.[98] Considering the privacy interference that takes place when law enforcement authorities obtain traffic data, the additional safeguard of an independent authority in the form of an investigative judge can indeed be considered appropriate. However, from a law enforcement perspective, the additional proce-

97 The Dutch legislature can still choose to force particular service providers to retain specific data for a certain amount of time for law enforcement purposes. How exactly new Dutch data retention legislation should look is beyond the scope of this research.

98 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 537, no. 3 (explanatory memorandum amended Data Retention Act), p. 2. Also note that the data retention period for internet data remains six months in the new proposal. Research shows that this retention period is not long enough for law enforcement authorities, as criminal investigations often take longer than six months (see Odinot et al. 2013, p. 118). Therefore, it is questionable whether the proposed amendment creates an effective data retention measure to ensure the availability of data that is required in criminal investigations. In cybercrime investigations, the data is most significantly IP addresses that can be linked to subscribers of a service (see also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 537, no. 3 (explanatory memorandum amended Data Retention Act), p. 5-7.

dural safeguard of a warrant may be regarded as undesirable, as a warrant requirement poses a significant administrative burden on law enforcement authorities. As a result, criminal investigations may be delayed. Public prosecutors must already assess whether obtaining data is in the interest of a particular investigation, which entails first determining how much data is appropriate considering the interests of that investigation. An investigative judge could play an important role in this process if he is required to confirm both that the public prosecutor has conducted a proper assessment and that the restrictions regarding the amount of information are appropriate (for example, based on time restrictions in relation to applying the warrant).[99] Considering both the intrusiveness of the investigative method and CJEU case law, the involvement of an investigative judge (through a warrant requirement) remains appropriate (*Recommendation 2*).

6.4.4 Other data

Other data consists of information that is not subscriber, traffic, or content data. The Dutch legislator should clarify that stored documents available at online service providers are to be equated with stored private messages and thus considered as content data. It is necessary to create clear lists that specify what constitutes (1) subscriber data, (2) traffic data, and (3) content data. By default, these lists would also reveal what the (broad) category of (4) other data entails. Such lists can be created and implemented in lower regulations.[100] In addition, a warrant from an investigative judge is also desirable for data production orders concerning other data, due to the investigative method's intrusive nature (*Recommendation 3*).

6.4.5 Content data

The DCCP currently provides an accessible legal framework for data production orders with regard to content data. However, it is desirable that the Dutch legislature extends the special investigative power to obtain e-mail and other private messages that are stored at online service provider to different types of content data (*Recommendation 4*). As explained in subsection 6.2.2, a discussion is taking place with regard to whether data related to (a) search terms, (b) links to websites, (c) domain names, and (d) subject lines in private messages must be considered content or traffic data (see Koops

99 Investigative judges already play a role in reviewing privileged communications from lawyers that are obtained after seizure by public prosecutors. See the guideline for the application of special investigative powers and compulsory measures in law firms (Stcrt. 2011, 4981). See also Mevis, Verbaan & Salverda 2016, p. 61-62. I suggest increasing the supervisory role of investigative judges in this respect.

100 See also the letter regarding the contours of the 'Modernising Criminal Procedural Law' project of 30 September 2015, p. 10-11. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (last visited on 23 March 2016).

& Smits 2014, p. 93-106).[101] In 2015, a good attempt was made to define content data in the explanatory memorandum of the new (concept) data retention bill, namely by stating that *"(a) the contents of conversations, messages or e-mails, (b) typed in search terms and (c) IP addresses of requested websites"* should qualify as content data.[102] The amended Data Retention Act of 2016 specifies that destination IP addresses and other 'surfing behaviours', concerning information about which websites are visited, are not retained under the proposed legislation.[103]

As argued in subsection 6.4.4, stored documents at online service providers (or other third parties) should also be considered content data. When art. 126ng(2) DCCP is applied to using data production orders to collect content data, the law is of sufficient quality. However, this particular special investigative power can be improved by both articulating the special investigative power more clearly and referring to content data as a separate category of data. First, a public prosecutor must determine how much data is required and balance that need with the interest of the investigation. Second, an investigative judge can determine whether that balance has been correctly assessed and verify the restrictions regarding the amount of data for which a production order is issued.[104]

6.5 Chapter conclusion

The aim of this chapter was to determine how Dutch criminal procedural law should be improved to adequately regulate the issuing of data production orders to online service providers (RQ 4b). To answer the research question, the Dutch legal framework regulating data production orders for all four types of data (i.e., subscriber data, traffic data, other data, and content data) was investigated with regard to its (1) accessibility, (2) foreseeability, and (3) the quality of the law.

The analysis has shown that – to a large extent – data production orders to obtain data from online service providers are regulated in an accessible manner. However, the foreseeability of data production orders and the quality of the law can be significantly improved for all types of data production orders. The results of the analysis are summarised in subsection 6.5.1. An overhaul of the legal regime for data production orders is required to improve the Dutch legal framework. Specific recommendations are provided in subsection 6.5.2.

---

101 With reference to Asscher & Ekker 2003, p. 104, Koops 2003, p. 77-78, Smits 2006, p. 416, Steenbruggen 2009, p. 56.

102 See p. 8 of the concept bill on data retention (2015).

103 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 537, no. 3 (explanatory memorandum amended Data Retention Act), p. 2.

104 For example, software filters can be used to select privileged communications or documents.

6.5.1 Summary of conclusions

Section 6.1 presented an analysis of the accessibility of the legal basis for the investigative method. That analysis revealed that a detailed and dual legal regime for data production orders exists in Dutch criminal procedural law. The legal framework for data production orders is regarded as accessible, since an adequate indication is provided concerning the applicable regulations to obtain subscriber data, traffic data, other data, and content data.

The analysis in section 6.2 made it clear that the dual regime for data production orders cannot be considered foreseeable. The reason is the ambiguity that exists with regard to which special investigative power applies for obtaining the identified types of data from online service providers. It is also unclear exactly which data should be considered traffic data, other data, and content data. Stated differently, there is a substantial lacuna in Dutch law concerning both the 'Who-question' (To whom can data production orders be issued and on which legal basis?) and the 'What-question' (What data can be obtained with the data production order regulated as a special investigative power in Dutch law?). These questions should be addressed in an amended legal regime for data production orders that preferably has just one tier of regulations.

The analysis in section 6.3 showed that within the Dutch legal framework, only the regulation of data production orders with regard to subscriber data meets the desired quality of the law. The regulations for data production orders concerning the categories of traffic data and other data do not require the involvement of an investigative judge, although such involvement is desirable. The special investigative power to obtain content data using data production orders also fails to meet the desired quality of the law, because it is unclear whether the special investigative power also requires a warrant to obtain stored documents from online service providers. Dutch law should be amended to meet the desirable quality of the law.

6.5.2 Recommendations

Section 6.4 provides four recommendations to improve the Dutch legal framework for data production orders. These recommendations follow the analysis of the adequacy of the Dutch legal framework based on the three normative requirements in section 6.1 to 6.4. These recommendations are as follows.

1. The current dual regime for data production orders in Dutch criminal procedural law should be merged into a single regime. Each category of data (except 'other data') should be specified in a list. This would render the legal framework less complex and thus improve both the accessibility, foreseeability, and the quality of the law.
2. The Dutch legal framework should be amended to incorporate a warrant requirement for collecting traffic data using data production orders.

3. The Dutch legal framework should be amended and also incorporate a warrant requirement for collecting other data using data production orders.
4. The Dutch legislature should clarify what data is included in the category of content data and require a warrant for the corresponding data production order.

7 Applying undercover investigative methods online

This chapter aims to answer the fourth research question with regard to online undercover investigative methods (RQ 4c): *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate online undercover investigative methods?* In this study, online undercover investigative methods are categorised as (1) online pseudo-purchases, (2) online undercover interactions with individuals, and (3) online infiltration operations. To answer the research question, the investigative method is placed within the Dutch legal framework and further analysed to determine whether the normative requirements of art. 8 ECHR for regulating investigative methods are fulfilled. In chapter 3, the normative requirements were identified as follows: (1) accessibility, (2) foreseeability, and (3) the quality of the law.

In chapter 4, the desirable quality of the law for online undercover investigative methods was formulated. Undercover investigative methods should be regulated in detail in statutory law with strong procedural safeguards to both ensure transparency in their application and prevent entrapment from taking place. Importantly, the ECtHR has articulated qualitative requirements for the domestic legal frameworks of contracting States to prevent entrapment from occurring and to ensure a fair trial as protected by art. 6 ECHR. These requirements are such that it is possible to transpose them to requirements for the *regulation* of undercover operations. Thus, although these requirements are based in art. 6 ECHR, they, or aspects of them, are similar to requirements that apply to interferences in the context of art. 8 ECHR. As such, it is taken as a point of departure that the art. 6 ECHR may be equated with art. 8 ECHR requirements. The Dutch legislator does recognise that interferences with the right to privacy take place when undercover investigative methods are applied and the requirements of art. 8(2) ECHR apply. This strengthens the argument to transpose the similar requirements derived from case law of art. 6 ECHR to the normative requirements derived from art. 8 ECHR.

Brief description of the Dutch legal framework for undercover operations

Before proceeding, it is important to examine the basics of the Dutch legal framework vis-à-vis undercover investigative methods. As explained in section 1.1, the Dutch IRT affair has been very influential in the regulation of (special) investigative methods in the Netherlands.[1] In the 1990s, law enforcement authorities took many liberties in deploying novel undercover

1 See also for an extensive analysis Blom 1998.

investigative methods to gather evidence in criminal investigations that were (mostly) related to drug crimes. The (secrecy surrounding the) utilisation of these undercover investigative methods and the use of authorised drug transports led to controversy in the Netherlands. The special parliamentary inquiry commission Van Traa was instated and delivered an extensive report regarding the use of these undercover investigative methods. The report included recommendations for new regulations. These recommendations eventually led to the Special Investigative Powers Act, which was adopted in 1999.[2]

With the implementation of this act in the DCCP in February 2000, the Dutch legislature created detailed regulations for, amongst other special investigative powers, the application of undercover investigative methods in Dutch criminal procedural law. The following undercover investigative methods were regulated as special investigative powers in the DCCP:

(1) The special investigative power to conduct a pseudo-purchase or pseudo-service (e.g., buying goods or providing services for evidence gathering purposes);
(2) The special investigative power for systematic information gathering (e.g., interacting with suspects while undercover); and
(3) The special investigative power for infiltration operations (e.g., undercover operations in criminal organisations).[3]

The Dutch legislator held that detailed regulations were necessary for these undercover investigative methods, because these methods (1) interfere with the rights and freedoms of the individuals involved in more than a minor manner and (2) endanger the integrity of criminal investigations.[4] The Dutch regulations for undercover investigative methods are illustrated in Figure 7.1 by plotting them on the scale of gravity for privacy interferences and accompanying quality of the law that is derived from art. 8 ECHR.

2 See section 1.1.

3 At the same time, many other special investigative powers were implemented in the Dutch criminal procedural legal framework. For an extensive analysis of these special investigative powers, see, for example, Buruma 2001, p. 33-130.

4 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 3 and 10.

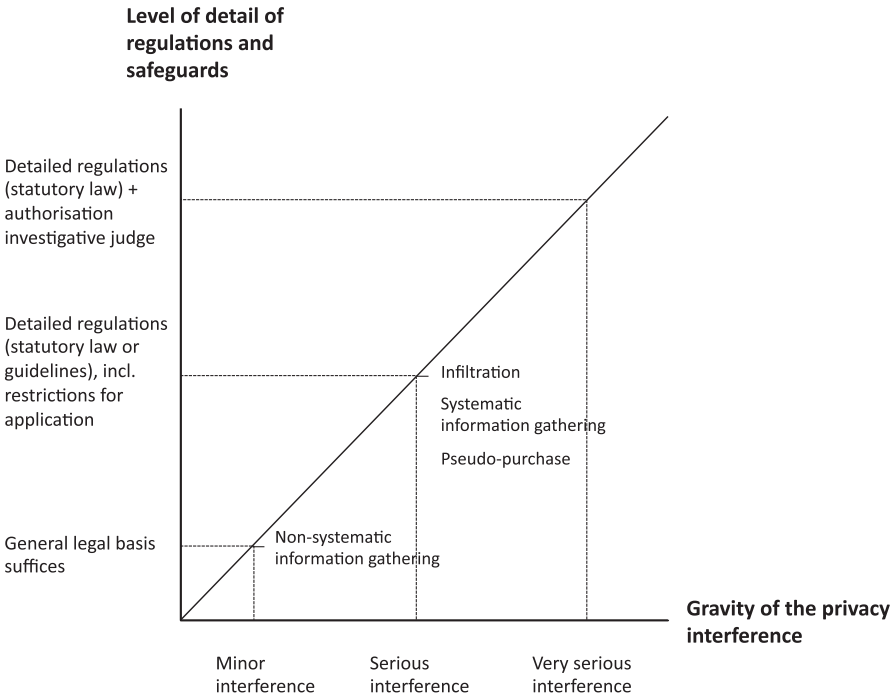

Figure 7.1: The Dutch scale of gravity for the regulation of undercover investigative methods.

Figure 7.1 illustrates how the level of detail and procedural safeguards for undercover investigative methods varies and depends on the gravity of the privacy interference which are different for each investigative method. It is worth noting that the Dutch legislature does not require a specific provision for all undercover investigative methods. Most notably, for non-systematic information gathering, the general legal basis in art. 3 of the Dutch Police Act may suffice. In this chapter, the Dutch legal framework for undercover investigative methods is thus tested with regard to accessibility, foreseeability, and the desired quality of the law.

Structure of the chapter

This chapter is structured as follows. The three normative requirements of art. 8(2) ECHR are tested in separate sections, each of which discusses all three types of undercover investigative methods. To assess the accessibility and foreseeability of the Dutch legal framework with regard to the investigative methods, the same scheme of research is used as in chapters 5 and 6. That research scheme entails examining the following four sources of law: (A) statutory law, (B) legislative history, (C) case law, and (D) public guidelines. Thereafter, the requirements for regulations extracted from art. 8 ECHR in chapter 4 are compared to the Dutch legal framework. Based on the results of the analyses, recommendations are provided to improve the Dutch legal framework.

It thus follows that section 7.1 tests the *accessibility* of the Dutch regulations for online undercover investigative methods. Section 7.2 examines the extent to which online undercover investigative methods are regulated in a *foreseeable* manner in the Netherlands. Section 7.3 analyses whether the Dutch legal framework for online undercover investigative methods meets the *desired quality of the law*. Based on the analyses in sections 7.1 to 7.3, section 7.4 provides concrete proposals as to how Dutch criminal procedural law can be improved to adequately regulate online undercover investigative methods. Section 7.5 concludes the chapter by presenting a summary of its findings.

7.1 Accessibility

An accessible basis in law means that the individual involved has an adequate indication of which regulations apply to the use of investigative methods in a particular case.[5] Given the detailed regulations that have been created for undercover investigative methods in the Netherlands, it is expected that this normative requirement will be unproblematic in Dutch law. However, whether the examined legal sources in law also indicate the legal basis for the *online* application of undercover investigative methods in the Netherlands must be explored separately.

Subsections 7.1.1 to 7.1.3 examine the accessibility of the three types of online undercover investigative methods. Subsection 7.1.4 then presents conclusions regarding the investigative method's accessibility in Dutch law.

7.1.1 Online pseudo-purchases

An online pseudo-purchase entails the investigative method during which an undercover law enforcement official poses as a potential buyer of an illegal good or data in order to gather evidence of a crime. For example, law enforcement officials may buy stolen data, drugs, or weapons from vendors in online forums to collect evidence in a cybercrime investigation.[6] The accessibility of the legal basis for applying online pseudo-purchases as an investigative method is examined below with the previously mentioned research scheme.

A Statutory law

In Dutch criminal procedural law, (online) pseudo-purchases are regulated by the special investigative power for pseudo-purchase.[7] Art. 126i(1) DCCP reads as follows.

5 See subsection 3.2.2 under A.
6 See subsection 2.2.3 under C.
7 See art. 126i DCCP.

"In case of reasonable suspicion of a crime as defined in art. 67 DCCP, first paragraph, a public prosecutor can order, insofar it is in the interest of the investigation, a law enforcement official to:
a. buy goods from a suspect;
b. buy data from a suspect that is stored, processed or transferred by an automated device through the intermediary of public telecommunication network, or
c. provide services to a suspect."

The special investigative power thus indicates that law enforcement officials can buy goods or data in a criminal investigation as part of an online pseudo-purchase as an investigative method. The technological neutral manner the provision is articulated provides room to conduct a pseudo-purchase in an online context when this special investigative power is applied. These detailed regulations in the DCCP are thus considered accessible to the individuals involved.

It should be noted that the special investigative power in art. 126i(1) DCCP also authorises law enforcement officials to provide services to a suspect in a criminal investigation.[8] This application of the investigative method is not examined in this study, since the identified digital investigative method focuses on purchasing goods or data from a suspect in an online context.[9]

B Legislative history

The Special Investigative Powers Act mandated that the investigative method of a pseudo-purchase be regulated in detail as a special investigative power.[10] The explanatory memorandum to the act specifies that this special investigative power allows for the one-time application of a pseudo-purchase in a criminal investigation.[11]

In 1997, the Dutch legislature also stated for the first time that special investigative powers can be applied 'on the Internet'.[12] This position was reiterated in the explanatory memorandum to the Computer Crime Act II in 1999. Here, the Dutch legislator stated that undercover investigative methods can be applied 'in the digital world'.[13]

8 See art. 126i(1) DCCP under c.
9 This does not mean that the investigative method is not relevant. See, e.g., Rb. Haarlem 8 September 2011, ECLI:NL:RBHAA:2011:BS8878, in which an online pseudo-service was conducted by responding to an offer of a money mule recruiter on a chat website. Based on the examination of case law on rechtspraak.nl (a database for judgements that were uploaded by Dutch courts), it appears that case law with regard to pseudo-services in an online context is scarce.
10 In art. 126i DCCP and art. 126ij DCCP (see the statutory law as examined above under A).
11 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 76.
12 In 1997, the Dutch legislature made clear that the special investigative powers for systematic information gathering and infiltration can be employed on the Internet in 'digital investigations' (*Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29 and p. 55.
13 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36-37.

The Computer Crime Act II amended the special investigative power for pseudo-purchase in order to enable law enforcement officials to purchase *data* as part of a pseudo-purchase.[14] This was done because the special investigative power previously only enabled law enforcement officials to purchase a good – and not data – from an individual involved in a criminal investigation. The amendment enables law enforcement officials to conduct a criminal investigation by, for instance, purchasing stolen login credentials offered by individuals in an online black market.

Dutch legislative history thus does indicate which regulations apply to this investigative method in Dutch law.

C Case law

A large amount of case law indicates that the investigative method of a pseudo-purchase is applied relatively often in an online context.[15] This case law is further explored in subsection 7.2.1 to examine the foreseeability of the investigative method. The case law affirms that law enforcement officials use the special investigative power in art. 126i DCCP to apply online pseudo-purchases as an investigative method in practice.

D Public guidelines

The Guideline for Special Investigative Powers affirms the detailed legal basis in Dutch criminal procedural law for using a pseudo-purchase as an investigative method. It does not specifically state that the investigative method can be applied in an online context.

7.1.2 Online undercover interactions with individuals

Performing online undercover interactions with individuals as an investigative method can take place on many online platforms, including chat services, private messaging services, social media services, discussion forums, and black markets. With the right knowledge of internet subcultures, law enforcement officials can interact and build relationships with individuals using credible fake identities in order to gather evidence in criminal inves-

14 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 37-39.

15 See Rb. Den Haag 10 July 2008, ECLI:NL:RBSGR:2008:BD7012 (online pseudo-purchase of soft drugs on a Dutch website), Rb. Roermond 4 March 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudo-purchase of suspected stolen goods at the online marketplace Marktplaats.nl), Rb. Zutphen, 28 January 2011, ECLI:NL:RBZUT:2011:BP2308 (online pseudo-purchase of illegal weapons), Rb. Haarlem 8 September 2011, ECLI:NL:RBHAA:2011:BS8878 (online pseudo service by responding to an offer of a money mule recruiter on a chat website), Rb. Oost-Brabant 6 May 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudo-purchase of illegal fireworks), Rb. Overijssel, 24 February 2014, ECLI:NL:RBOVE:2014:884 (online pseudo-purchase of illegal fireworks), Rb. Rotterdam 8 May 2014, ECLI:NL:RBROT:2014:3504 (online pseudo-purchase on the drug trading website Silk Road), and Rb. Overijssel, 18 April 2016, ECLI:NL:RBOVE:2016:1323 (online pseudo-purchase of ivory from endangered species).

tigations (cf. Siemerink 2000b, p. 145 and Petrashek 2010, p. 1528).[16] The accessibility of the legal basis for using online undercover interactions with individuals as an investigative method is examined below utilising the announced research scheme.

A Statutory law

Dutch statutory law only provides a detailed legal basis for *systematically* performing undercover interactions with individuals as an investigative method within a criminal investigation. Art. 126j(1) DCCP reads as follows.

"In case of reasonable suspicion of a crime, a public prosecutor can, insofar it is in the interest of the investigation, order a law enforcement official as meant in art. 141(b) DCCP, to systematically gather information about the suspect, without being recognisable as a law enforcement official."

The text of the special investigative power thus indicates that a law enforcement official can systematically gather information about the suspect, without being recognisable as a law enforcement official. The text itself does not suggest that the investigative method includes the undercover *interactions* with individuals, but it does not exclude this option either. An accessible legal basis is therefore provided for the systematic application of this investigative method. The special investigative power in art. 126j(1) DCCP does not mention the investigative method can be applied in an online context. However, the text does not exclude the possibility either.

From the system behind the regulation of investigative methods in Dutch criminal procedural law (see the introduction to chapter 5), it follows that the basis for undercover interactions with individuals is derived from either (1) the description of the statutory duty of law enforcement officials to investigate crime set forth in art. 3 of the Dutch Police Act or (2) the above-mentioned special investigative power for systematic information gathering.[17]

B Legislative history

The Dutch legislature explicitly mentioned in its explanatory memoranda to the Special Investigative Powers Act and the Computer Crime Act II that the special investigative power for systematic information gathering can also be applied on the Internet.[18] The explanatory memorandum to the Special Investigative Powers Act explains that law enforcement officials who systematically gather information about a suspect *actively interfere* in that suspect's

16 See subsection 2.2.2 under C.

17 See (1) art. 3 Dutch Police Act 2012 in combination with 141-142 DCCP and (2) art. 126j DCCP.

18 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 34. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 37.

life. Their activities go beyond mere observation or listening in on conversations.[19] This description meets the digital investigative method of undercover online interactions with individuals that are involved in a criminal investigation. Dutch legislative history thus provides an indication of the applicable regulations for applying this investigative method in an online context.

C Case law

Until 10 December 2015, no Dutch case law provided an indication of the applicable legal basis for the investigative method of online undercover interactions with individuals. However, on that date, the Court of The Hague provided the first judgment in the Netherlands about the appropriate legal basis for a specific application of this investigative method and affirmed that the special investigative power of systematic information gathering can be applicable to undercover online interactions with individuals involved in a criminal investigation.[20] The facts of the case are further considered in subsection 7.2.1 to illustrate the scope of the investigative method and the manner in which the investigative method can be applied.

D Public guidelines

The Guideline for Special Investigative Powers of the Public Prosecutors Service from 2014 does not discuss the *online* application of the investigative method that involves undercover interactions with individuals in a criminal investigation.

However, it does state that the legal basis for applying this investigative method in the physical world is derived from either (1) the statutory duty of law enforcement officials to investigate crime in art. 3 of the Dutch Police Act or (2) the special investigative power for systematic information gathering. Furthermore, the guideline specifies how the investigative power is to be differentiated from other special investigative powers that regulate other undercover investigative methods. The guideline explains that the special investigative power differs from systematic observation in the sense that the systematic information gathering is not limited to the following or observing the behaviours of an individual, but also authorises a law enforcement to *actively interfere* in the life of the individual involved to gather evidence.[21]

7.1.3 Online infiltration operations

Infiltration operations are similar to undercover interactions with individuals. However, the former are distinguished in this study by the fact that undercover agents involved in these operations are authorised (to a certain

19 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 35.

20 Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, m.nt. J.J. Oerlemans, *Computerrecht* 2016, no. 2, p. 113-124.

21 See section 2.6 of the Guideline for Special Investigative Powers.

extent) to *participate* in a criminal organisation. This may entail, for instance, participating in a criminal organisation that is active within an online black market. Infiltration operations have in common with a pseudo-purchase that a(n) (authorised) crime can be committed during their application.

The accessibility of the legal basis for applying an online infiltration operation as an investigative method is examined below using the announced research scheme.

A Statutory law

In Dutch criminal procedural law, infiltration operations are regulated by the special investigative power for infiltration. Art. 126h(1) DCCP reads as follows.

"In case of reasonable suspicion of a crime as defined in art. 67 DCCP, first paragraph, which considering its nature or cohesion with other crimes committed by the suspect seriously interfere with the legal order, a public prosecutor can, insofar the interest of investigation demands it, order a law enforcement official as meant in art. 141(b) DCCP to participate in or provide services to a group of persons that are reasonably suspected of committing or plotting crimes".

These specific regulations provide an indication of the legal basis for this investigative method, because it enables law enforcement officials (under stringent conditions) to participate in or provide services to an organised crime group.

B Legislative history

In its explanatory memorandum to the Special Investigative Powers Act in 1997, the Dutch legislator explicitly stated that the special investigative power for infiltration can also be applied 'on the Internet'.[22] This statement was repeated in the explanatory memorandum to the Computer Crime Act II in 1999.[23] The Dutch legislator noted in its explanatory memorandum to the earlier act that the special investigative power is considered necessary given that the investigative method enables law enforcement officials to infiltrate a criminal organisation to both collect evidence about the crimes that the organisation is committing (or preparing to commit) and gain insights into its modus operandi.[24] Dutch legislative history thus provides an indication regarding the legal basis for this investigative method.

22 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29.

23 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36-37.

24 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 28.

C Case law

Case law that involves the use of infiltration as a special investigative power in an online context is rare in the Netherlands. *One* available case specifies that the special investigative power for infiltration has been used on the Internet.[25] The details of this case are further examined in subsection 7.2.3 in order to analyse the scope of the investigative method and the manner in which the investigative method is applied in practice.

D Public guidelines

The Guideline for Special Investigative Powers does not specify that infiltration operations can also be applied in an online context. It instead merely repeats legislative history by specifying the legal basis for the special investigative power for infiltration.[26]

7.1.4 Section conclusion

The accessibility of the Dutch legal framework in criminal procedural law with regard to online undercover investigative methods can be assessed based on the analyses conducted in subsections 7.1.1 to 7.1.3, the results of which are presented below.

The online undercover investigative method are in their application similar to the application of undercover investigative method in the physical world (although they are applied in a different context). In order words, the investigative methods match and do not require regulations in special provisions in the DCCP.

Performing a pseudo-purchase as an investigative method is regulated as a special investigative power in Dutch law. Dutch legislative history and case law make it clear that this special investigative power for pseudo-purchase can also be applied in an online context. For that reason, the Dutch legal basis for this investigative method is considered *accessible*.

The systematic application of interacting with individuals in an undercover capacity is regulated by the special investigative power for systematic information gathering in the DCCP. It follows from the Dutch system for regulating investigative methods in criminal procedural law that the non-systematic application of this investigative method can be based on the statutory duty of law enforcement officials to investigate crimes set forth in art. 3 of the Dutch Police Act. Dutch legislative history and case law make it clear that the special investigative power can also be applied in an online context. For that reason, the Dutch legal basis for the investigative method is considered *accessible*.

25 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792.

26 See section 2.6 and 2.9 of the Guideline for Special Investigative Powers.

Infiltration operations are regulated by the special investigative power for infiltration in the DCCP. Legislative history and case law make clear that the special investigative power can also be applied in an online context. Therefore, the legal basis in the DCCP for this investigative method is considered *accessible*.

7.2 Foreseeability

A legal framework that is foreseeable prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which an investigative method is exercised.[27] The analysis in section 7.1 has shown that Dutch law provides a detailed legal framework that indicates which legal basis applies to the identified digital investigative methods. With the corresponding regulations, the Dutch legislature aimed to provide an accessible and foreseeable legal framework that enables the individuals involved in undercover operations to foresee when and how undercover investigative methods can be applied.[28] The analysis below determines whether that objective is achieved in terms of foreseeability.

Subsections 7.2.1 to 7.2.3 examine the foreseeability of all three types of online undercover investigative methods. Subsection 7.2.4 then presents conclusions regarding the foreseeability of this investigative method in Dutch law.

7.2.1 Online pseudo-purchases

The foreseeability of the regulations for applying online pseudo-purchases as an investigative method is examined below using the announced research scheme.

A Statutory law

The special investigative power that regulates pseudo-purchases in detail in art. 126i DCCP indicates the scope of the investigative method and the manner the special investigative power is applied by stating the requirements that Dutch law enforcement officials must meet to purchase goods or data from a suspect. The investigative power can only be applied in the interest of criminal investigations involving crimes as defined in art. 67(1) DCCP, after authorisation is obtained from a public prosecutor.[29]

27 See subsection 3.2.2 under B.

28 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 10.

29 See art. 126i(1)DCCP.

The special investigative power also explicitly incorporates the prohibition of entrapment in art. 126i(2) DCCP.[30] The prohibition of entrapment also restricts the scope of the investigative method and the manner the investigative method can be applied. The Netherlands essentially has the same understanding of entrapment as the ECtHR. In 1991, the Dutch Supreme Court made it clear in the *Tallon* case that Dutch law enforcement authorities must ensure that 'a civilian does not commit a crime that would not have been committed without the intervention of law enforcement authorities'.[31] As noted in subsection 4.3.1, the ECtHR also requires that an offence would have been committed without the intervention of law enforcement authorities (cf. Ölçer 2014, p. 16).[32] An undercover operation should therefore remain 'essentially passive'. Law enforcement authorities should merely 'join' criminal acts that have already commenced and not instigate them.[33] Whether entrapment has taken place is decided on a case-by-case basis.

Statutory law itself thus provides on indication regarding the scope of the investigative method and the manner in which the investigative method is applied.

B Legislative history

The explanatory memorandum to the Special Investigative Powers Act specifies the manner in which this investigative can be applied in the physical world. The legislative history states that the special investigative power allows law enforcement officials to commit crimes, such as purchasing a weapon, as part of a criminal investigation.[34] The explanatory memorandum states explicitly that the special investigative power does not authorise a law enforcement official to sell an illegal good and then arrest the purchaser.[35]

---

30 Art. 126i(2) DCCP reads as follows: "*The investigating law enforcement official that applies the order shall not bring a suspect to commit other offences than those that he intended to commit*".

31 See HR 4 December 1979, ECLI:NL:HR:1979:AB7429, *NJ* 1980, 356, m.nt. Th.W. van Veen. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 31.

32 See ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, § 36-46 for an extensive test to determine whether police entrapment has taken place.

33 ECtHR 4 November 2010, *Bannikova v. Russia*, App. no. 18757/06, §43. See also ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09 § 50. To determine whether law enforcement authorities interfered in an active manner that led the suspect to committing the offence, the ECtHR takes the following four factors into consideration: (1) the reasons underlying the undercover operation, (2) the behaviour of the law enforcement authorities, (3) the existence of a reasonable suspicion that the suspect was involved in criminal behaviours, and (4) the suspect's predisposition to the crime (see Ölçer 2014, p. 16 and ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, *EHRC* 2011/9, m.nt. Ölçer).

34 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 34.

35 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 34. It is noted in the explanatory memorandum that such an application will likely entail entrapment.

The explanatory memorandum to the Computer Crime Act II provides the example of a law enforcement official being able to purchase illegal software or child pornography in order to gather evidence in a criminal investigation.[36] Legislative history thus provides an indication about the manner in which this investigative method is applied.

C Case law

Case law indicates that Dutch law enforcement officials have used this special investigative power to purchase a wide variety of goods that were offered on the Internet. Examples of these goods include drugs, fireworks, weapons, stolen items, and even ivory obtained from endangered animal species.[37] It should observed here that a much greater amount of case law is available regarding this investigative method than for other digital investigative methods that are examined in this study. A report that evaluated the use of undercover investigative methods in the Netherlands also explicitly noted that the special investigative power for pseudo-purchase is often applied in an online context in criminal investigations (Kruisbergen & De Jong 2010, p. 216). Dutch case law thus provides a good indication about the manner in which this investigative method is practically applied in the Netherlands.

The cases show that before a pseudo-purchase is conducted, law enforcement officials contact (and thus interact undercover with) the suspect by e-mail, telephone, or an online private messaging system, in order to reach agreement to purchase the good. These cases have in common that the judges find that the application of the special investigative power of pseudo-purchase is appropriate in the situation that law enforcement officials first contacts the suspect that offers (illegal) goods on an online trading platform in order to purchase that good. The application of the special investigative power does not require that the goods are necessarily delivered to law enforcement officials; it applies as soon as the interaction with the suspect

36 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 38.

37 See Rb. Den Haag 10 July 2008, ECLI:NL:RBSGR:2008:BD7012 (online pseudo-purchase of soft drugs on a Dutch website), Rb. Roermond 4 March 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudo-purchase of suspected stolen goods at the online marketplace Marktplaats.nl), Rb. Zutphen, 28 January 2011, ECLI:NL:RBZUT:2011:BP2308 (online pseudo-purchase of illegal weapons), Rb. Oost-Brabant 6 May 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudo-purchase of illegal fireworks), Rb. Overijssel, 24 February 2014, ECLI:NL:RBOVE:2014:884 (an online pseudo-purchase of illegal fireworks), Rb. Rotterdam 8 May 2014, ECLI:NL:RBROT:2014:3504 (online pseudo-purchase on the drug trading website Silk Road), and Rb. Overijssel, 18 April 2016, ECLI:NL:RBOVE:2016:1323 (online pseudo-purchase of ivory from endangered species). See also Landelijk Parket, 'Undercover onderzoek naar illegale marktplaatsen op internet', 12 February 2014, Landelijk Parket. Available at: https://www.om.nl/vaste-onderdelen/zoeken/@32626/undercover-onderzoek/ (last visited on 17 April 2015).

starts to purchase the good.[38] In two of the seven cases, law enforcement officials asked for authorisation of a public prosecutor too late in the operation, i.e., after the undercover law enforcement officials contacted the suspect or after the agreement to purchase the goods were made.[39]

D Public guidelines

The Guideline for Special Investigative Powers provides detailed information (more than for other investigative methods) about the scope of the special investigative power for pseudo-purchase and the manner in which this power is applied.[40] For example, it explains how law enforcement officials can use this special investigative power to (1) maintain their cover, (2) determine whether a suspect indeed offers an illegal good, and (3) determine the quality of the good (such as a drug) being offered.

The guideline also states that – although the explanatory memoranda to the Special Investigative Powers Act and the Computer Crime Act II do not restrict the investigative power to certain goods – it is not desirable to purchase particular goods. For instance, a public prosecutor cannot authorise the purchase of human organs as part of a pseudo-purchase. In 2011, a report of the Dutch national rapporteur on human trafficking mentioned that Dutch law enforcement authorities do not find it desirable to distribute child pornography on the Internet, as doing so perpetuates the psychological abuse of the minors involved.[41] Considering this, it can be argued that it is also not desirable to purchase child pornography since doing so can stimulate the 'child pornography market'. At the same time, however, purchasing child pornography on the Internet can be an important way to identify abused children and possibly obtain evidence about crimes that are being committing (e.g., child abuse and the distribution of child pornography).

7.2.2 Online undercover interactions with individuals

The foreseeability of regulations for online undercover interactions with individuals as an investigative method is examined below using the announced research scheme.

---

38 See, e.g., Rb. Roermond 4 March 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudo-purchase of suspected stolen goods at the online marketplace Marktplaats.nl) with reference to HR 30 September 2003, ECLI:NL:HR:2003:AF7331, *NJ* 2004, 84 m.nt. Y. Buruma and and Rb. Oost-Brabant 6 May 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudo-purchase of illegal fireworks).

39 See Rb. Roermond 4 March 2009, ECLI:NL:RBROE:2009:BH4757 and Rb. Oost-Brabant 6 May 2013, ECLI:NL:RBOBR:2013:BZ9467. The procedural defect was not sanctioned, because the suspect already offered the good on an online trading platform and law enforcement officials discussed the application of the investigative method with the public prosecutor.

40 See most notably section 2.8 of the guideline.

41 See p. 164-165 of the 2011 report of the Dutch national rapporteur on human trafficking (Nationaal Rapporteur Mensenhandel (2011). Kinderpornografie – Eerste rapportage van de nationaal rapporteur. Den Haag: BNRM).

A Statutory law

The special investigative power for systematic information gathering in art. 126j DCCP states that law enforcement officials can 'systematically gather information about the suspect, without being recognisable as a law enforcement official'.[42] The wording of the special investigative power itself therefore does not restrict the scope of the investigative method, except in the sense that it refers to the *systematic* gathering of information about a suspect.

The special investigative power for systematic information gathering further specifies the requirements to apply this special investigative power, stating both that authorisation from a public prosecutor is necessary and that the investigative power can be used in criminal investigations regarding any type of crime.[43] This special investigative power can be applied for a maximum duration of three months.[44] The prohibition of entrapment is notably absent from the regulations associated with this special investigative power (cf. Ölçer 2014, p. 16). In contrast, the prohibition of entrapment is explicitly stated in the special investigative powers for pseudo-purchases and infiltration.[45] The explicit incorporation of the prohibition of entrapment clarifies the scope of the investigative method and the manner the investigative method can be applied, since it emphasises that entrapment is forbidden. The prohibition of entrapment is applicable nevertheless since it flows forth from art. 6 ECHR.

B Legislative history

Dutch legislative history provides more information regarding the scope of this investigative method and the manner in which the investigative method is applied.

As noted in subsection 7.1.2 under B, the explanatory memorandum to the Special Investigative Powers Act explains that law enforcement officials who systematically gather information about a suspect *actively interfere* in that suspect's life. Their activities go beyond mere observation or listening in on conversations.[46] The explanatory memorandum also states that the special investigative power for systematic information gathering is formulated in a technological neutral manner to enable law enforcement officials to conduct 'digital investigations'.[47]

The explanatory memorandum to the Computer Crime Act II also provides more information on the manner the special investigative power is applied. The legislative history states that that an undercover law enforcement official can interact with other individuals on the Internet in so-called

42 See subsection 7.2.1 under A.
43 See also subsection 7.1.2.
44 See art. 126j(2) DCCP.
45 See art. 126i(2) DCCP and art. 126h(2) DCCP.
46 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 35.
47 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p 5.

'newsgroups'.[48] In such a situation, a law enforcement official actively participates in a newsgroup by posting messages.[49] The explanatory memorandum emphasises that the investigative power is only applicable when the investigative method is applied systematically.[50]

It should be noted that the explanatory memoranda to both the Special Investigative Powers Act and the Computer Crime Act II do not further indicate when the application of undercover interaction with other individuals as an investigative method becomes 'systematic' in nature. This is important to know, as crossing that line means that it is appropriate to apply the special investigative power for systematic information gathering. Insofar as the investigative method is not systematically applied, the general legal basis in art. 3 of the Dutch Police Act suffices, which is not restricted to any type of crime or duration.[51]

When an undercover law enforcement official interacts with a suspect online, it must be determined at which point in the undercover operation the investigative method becomes systematic in nature. Questions that must be answered in this regard include the following: What factors apply when determining whether the investigative method is applied systematically? Does systematic application depend on the frequency of the online interactions or perhaps the duration of the investigative method? Does it make a difference if conversations are held on a specific type of communications service, such as e-mail or a chat program? Are law enforcement officials allowed to take over accounts of co-operating informants and interact with individuals involved in criminal investigations through those accounts? Overall, many questions concerning the application of this special investigative power in an online context remain unanswered in legislative history. I therefore conclude that the scope of the investigative method is not sufficiently foreseeable in the sense that it is not clear when the application of the method is to be considered systematic.

---

48 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 34. Wikipedia aptly describes a 'newsgroup' as a *"repository usually within the Usenet system, for messages posted from many users in different locations. Newsgroups are discussion groups, and are not devoted to publishing news, but were when the internet was young. Newsgroups are technically distinct from, but functionally similar to, discussion forums on the World Wide Web"*. Available at: http://en.wikipedia.org/wiki/Usenet_newsgroup (last visited on 8 April 2015). Newsgroups are frequently utilised to distribute and download (often copyrighted) music and videos. Newsgroups still exist. However, music and video files are today more often distributed through online peer-to-peer services or music and video streaming services.

49 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 37.

50 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 37.

51 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 115. However, one can argue that as part of the proportionality principle, undercover operations should *always* be restricted in duration.

C Case law

Only *one* case specifically deals with the appropriate legal basis when law enforcement officials gather evidence in a criminal investigation using undercover online interactions with individuals as an investigative method.[52] This case concerns a criminal investigation with regard to terrorist crimes, in which law enforcement officials used social media services to gather evidence about the suspects. The law enforcement officials created fake profiles on the social media service Facebook and then added themselves as 'friends' to the suspect's own online Facebook profile in order to learn more about the suspect and his activities.[53]

In its decision, the Court of The Hague first cites the relevant Dutch legislative history for the investigative method of systematic information gathering.[54] The court then takes a remarkable step by stating that the investigative methods of observation and information gathering are very similar.[55] In reality, the investigative methods are significantly different: the investigative power for systematic observation concerns the *passive monitoring* of people's behaviours, while the investigative power for systematic information gathering concerns *interacting with people* to gather evidence.[56] These special investigative powers do have in common that they only apply when the investigative method is being used *systematically*. However, the explanatory memorandum of the Special Investigative Powers only cites factors to determine when observation becomes systematic. As explained in subsection 5.2.3, these factors are (1) duration, (2) place, (3) intensity or (4) frequency, and whether (5) a technical device is used while observing an individual's behaviours.[57]

Nevertheless, in the judgment, the Court of The Hague used the same factors provided by the Dutch legislature to determine when observation becomes systematic in nature to determine when the information gathering becomes systematic in nature.[58] In my view, this can be explained by the fact that neither the Dutch legislator (in its legislation) nor the Dutch judiciary (in its consideration of earlier cases) has provided clarity as to when

52 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365.

53 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.1-5.40.

54 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.15-5.21.

55 In contrast to the application of the special investigative power for observation, the legislature provides no criteria for determining when application of the special investigative power for systematic information gathering is required. Cf. Melai and Groenhuijsen 2008, art. 126j DCCP, note 3.

56 See, e.g., section 2.6 of the guideline for special investigative powers of 2014.

57 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 26-27. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 7, p. 46.

58 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.22.

information gathering becomes systematic.[59] More clarity about which factors apply is required to identify when the investigative method becomes systematic and the special investigative power for systematic information gathering applies.

With regard to the 'online befriending operation' on Facebook in the aforementioned case, the Court of The Hague decided that the special investigative power for systematic information gathering should have been applied before an online account was created on the Facebook social media service.[60] This particular case therefore suggests that the use of the special investigative power for systematic information gathering is appropriate for an 'online befriending operation' that requires the creation of an account on a social media service in order to view the contents of a private profile and engage in discussions with a suspect for a period of three months. The case thereby provides an indication of the scope of the investigative method by specifying when the special investigative power is appropriate and explaining how the investigative method can be applied in practice.

D Public guidelines

The Guideline for Special Investigative Powers provides a significant amount of information regarding the manner in which this investigative method is practically applied in an offline context. It mentions that the investigative method becomes systematic in nature when 'more or less complete insights are obtained about certain aspects of an individual's private life'.[61] When this criterion is not met, law enforcement officials can use the investigative method based on the statutory duty of law enforcement officials to investigate crime.

---

59 Dutch courts use different criteria to determine whether the investigative method is applied systematically in the physical world. These factors can be identified as follows: (1) the manner in which the information is acquired, (2) the duration of the operation, (3) the location the information is collected from, and (4) the level of intensity of misdirection that is involved (see, e.g., Rb. Dordrecht 30 May 2002, ECLI:NL:RBDOR:2002:AE3709, Rb. Zwolle, 11 February 2003, ECLI:NL:RBZWO:2003:AF4427, Rb. Oost-Brabant, 30 January, ECLI:NL:RBOBR:2015:461). Nonetheless, these criteria are used in an inconsistent manner by Dutch courts (see also Van der Bel 2015 Sdu Commentary for art. 126j DCCP, at D and Buruma and Verborg in: De Melai & Groenhuijsen 2008 for art. 126j DCCP, at 3).

60 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.27. In this case, the law enforcement official who carefully constructed the online identity of a jihadist on Facebook should have requested a public prosecutor to authorise the online undercover operation in an earlier stage and should have reported the operation more carefully. The lack of prior authorisation from a public prosecutor and sloppy reporting were not sanctioned by the judges. See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.34-5.35 and 5.38-5.39. For my commentary regarding the case, see: Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, m.nt. J.J. Oerlemans, *Computerrecht* 2016, no. 2, p. 113-124.

61 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 26-27. This criterion is used to determine when observation as an investigative method becomes systematic in nature (see also subsection 5.2.3).

The guideline also indicates that when it is expected that law enforcement officials will systematically gather information from a suspect's surroundings using a false identity, it is appropriate to use a special police team to conduct the undercover operations.[62]

Finally, the guideline specifies how this special investigative power is different from other special investigative powers.[63] It explains that this special investigative power differs from the special investigative power for infiltration in the sense that in infiltration operations, law enforcement officials are authorised to commit crimes when participating in the criminal organisation.[64]

With regard to the *online* application of this special investigative power, it is relevant to know that the guideline provides no direction. This leaves many questions unanswered. Considering the opportunities that, for example, undercover operations on social media services provide to law enforcement officials, more explanation regarding the use of the special investigative power to systematically gather information in an online context seems appropriate. Due to this lack of information, the guideline does not – in my view – sufficiently indicate the scope of the investigative method when it is applied in an online context.

7.2.3 Online infiltration operations

The foreseeability of the regulations for online infiltration operations as an investigative method is examined below using the announced research scheme.

A Statutory law

The special investigative power for infiltration in art. 126h DCCP can be distinguished from the text of the special investigative power for systematic information gathering, in the sense that the special investigative power for infiltration focuses on *participating in* or *providing services to* an organised crime group.[65] The text of the special investigative power itself indicates the manner the investigative method is applies. It is notable that there is no such

62 In this respect, one can question whether these teams are fully equipped to perform online undercover operations, since they require knowledge about the relevant internet subcultures. However, this aspect is not further examined, as this study is not concerned with operational issues regarding the use of the investigative methods.

63 See section 2.6 of the guideline.

64 Confusingly, the guideline also states in section 2.7 that civilians under supervision of law enforcement authorities can deliver services to criminals, as long those services do not contribute the commission of the crime the suspect is suspected from.

65 The analysis in subsection 7.2.2 under D has shown that law enforcement officials can also provide services to a suspect using the special investigative power for systematic information gathering. The difference is that in infiltration operations, the service that is provided can facilitate the crime, whereas this is not possible when the special investigative power for systematic information gathering is applied.

thing as 'non-systematic' infiltration as an investigative method. As soon as the investigative method involves the participation or providing services to an organised crime group, the special investigative power of infiltration is applicable.

The special investigative power for infiltration further specifies stringent requirements that apply to this investigative power and therefore indicates the manner in which the investigative method is applied in practice.[66] The special investigative power for infiltration can only be applied in criminal investigations with regard to crimes as defined in art. 67 DCCP, that seriously infringe the legal order, and when necessary for furthering the investigation. A public prosecutor must authorise the use the special investigative power for infiltration.[67] The special investigative power also explicitly incorporates the prohibition of entrapment in art. 126h(2) DCCP. This provision further restricts the scope of the investigative method and the manner the investigative method is applied.

B Legislative history

The explanatory memorandum to the Special Investigative Powers Act extensively describes the regulation of infiltration as an investigative method in Dutch criminal procedural law.[68] This is unsurprising considering the events surrounding the IRT affair. Infiltration operations were one of the main investigative activities of law enforcement officials that led to the controversy in Dutch society concerning undercover operations. The Dutch legislature required legislation to regulate the use of undercover investigative methods, such as infiltration operations, in order to control the integrity of an investigation and protect the involved individuals' right to privacy.[69]

The explanatory memorandum to the Special Investigative Powers Act characterises this undercover investigative method as an undercover operation that entails *participating* in a criminal organisation.[70] The Dutch legislature noted that this special investigative power is considered necessary given that the investigative method enables law enforcement officials to infiltrate a criminal organisation to both collect evidence about the crimes it is committing (or preparing to commit) and gain insights into its modus

66 See subsection 7.1.3.

67 See art. 126h DCCP.

68 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 28-33.

69 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 3 and 10.

70 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29. See also the 2014 letter of the Dutch Minister of Security and Justice to the Dutch Parliament about the difference in 'informants' and 'individuals infiltrating criminal investigations' (8 October 2014, number 571620).

operandi.[71] Law enforcement officials are authorised to commit crimes in an infiltration operation. For example, they do not have to obtain separate authorisation from a public prosecutor to perform a pseudo-purchase as an investigative power. The special investigative power for infiltration thus also authorises the application of a pseudo-purchase as an investigative method.[72]

With specific regard to use of this special investigative power in an *online context*, the Dutch legislature explicitly notes in explanatory memoranda of the Special Investigative Powers Act and the Computer Crime Act II that law enforcement officials can also (virtually) infiltrate networks of individuals who distribute child pornography through the Internet.[73] However, the previously mentioned report of the Dutch national rapporteur on human trafficking states that Dutch law enforcement authorities do not find it desirable to participate in these networks, as they must distribute child pornography in order to gain access.[74] Doing so will perpetuate the psychological abuse of the minors involved.[75]

Finally, the explanatory memorandum to the Special Investigative Powers Act states that law enforcement officials are not allowed to sell illegal goods or provide illegal services as part of an infiltration operation.[76] However, they are permitted to assist a criminal organisation by setting up a 'front store'. A 'front store' (also known as a 'storefront') is a shop that law enforcement authorities set up in order to facilitate certain activities of a criminal organisation (cf. Corstens & Borgers 2014, p. 518). Legislative history indicates that a front store can for instance facilitate the transport of goods or the conversion of currency for money laundering purposes, with the aim of gathering evidence in a criminal investigation.[77] The explana-

71 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 28.

72 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 33.

73 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36-37. The explanatory memorandum to the Computer Crime Act II also states on p. 37 that the special investigative power can be applied on the Internet, which means that law enforcement officials can participate in or facilitate a criminal organisation that is active on the Internet.

74 See p. 164-165 of the 2011 report of the Dutch national rapporteur on human trafficking (Nationaal Rapporteur Mensenhandel (2011). Kinderpornografie – Eerste rapportage van de nationaal rapporteur. Den Haag: BNRM).

75 See subsection 7.1.3 under D.

76 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 119 (with the exception of small amounts of drugs).

77 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 31. With regard to the use of 'front stores', see also the Van Traa report (*Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1995/96, 24 072, nos. 10-11, p. 230 and 239-240).

tory memoranda to the Special Investigative Powers Act and the Computer Crime Act II do not cite any examples of the use of online front stores as part of the application of this special investigative power in an online context.[78] This raises the question of how using front stores translates to an online environment (cf. Siemerink 2000b, p. 143). In my view, it is also conceivable that Dutch law enforcement authorities could assist a criminal organisation with setting up a VPN connection as an anonymising service, while simultaneously wiretapping the connection to gather evidence.[79]

C Case law

Case law that deals with the legitimacy of the use of the special investigative power for infiltration in an online context is scarce. However, *one* case illustrates the scope of the investigative method and the manner in which the investigative method is applied.

In 2013, Dutch law enforcement officials *participated in an online drug-trading forum* as part of an online infiltration operation.[80] The criminal investigation focused on identifying the 'moderators' of a criminal online forum. Moderators generally manage the day-to-day affairs of a forum by scrutinising forum posts and forum users.[81] This particular drug-trading forum was only available through the Tor system and reportedly had 90,000 permanent users with an estimated monthly turnaround of nine million dollars. The moderators also sold drugs on the forum themselves.[82]

78 The explanatory memorandum to the Special Investigative Powers Act notes on p. 119 that the use of front stores is further regulated in internal guidelines.

79 See subsection 2.2.2, in which the 'DarkMarket-investigation' was described to illustrate an online infiltration operation. In that operation, an undercover agent worked himself up within an online forum that specialised in trading stolen credit cards. By providing a VPN service that was wiretapped by the FBI, U.S. law enforcement officials were able to gather evidence. See, e.g., Kim Zetter, 'TJX Hacker Gets 20 Years in Prison', *Wired*, 25 March 2010. Available at: https://www.wired.com/2010/03/tjx-sentencing/ (last visited on 20 February 2016).

80 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792. The court cryptically explains that the suspects made use of a 'secured network' to 'anonymously' buy and sell drugs on online market places. The suspects likely made use of the Tor network to buy and sell drugs on hidden services, more specifically 'Black Market Reloaded' and 'Utopia'. See *ANP*, 'OM wil tot zeven jaar cel voor internetdealers', *Nu.nl*, 23 September 2014. Available at: http://www.nu.nl/internet/3885624/wil-zeven-jaar-cel-internetdealers.html (last visited on 17 April 2015). See also J.J. Oerlemans, 'Veroordelingen voor drugshandel via online marktplaatsen', *Computerrecht* 2015, no. 3, p. 170.

81 See Wikipedia, 'Internet forum'. Available at: http://en.wikipedia.org/wiki/Internet_forum#Moderators (last visited on 16 April 2015).

82 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792. Interestingly, the authorisation to infiltrate the criminal investigation also encompassed the use of a foreign undercover agent.

Dutch law enforcement authorities aimed at becoming a 'moderator' within this online drug-trading forum, in order to gather evidence about drug dealers who were active in it. In order to achieve this goal, the officials applied the following special investigative powers:

(1) Systematic information gathering (to enable online interactions with the moderators);
(2) A pseudo-purchase of drugs (to enable the purchase and tracking of drugs deals from the online market place);
(3) Systematic observation (to enable the investigative method to observe a suspect's movements in the physical world); and
(4) Infiltration (to enable the officials' (eventual) participation in the online forum as a moderator).[83]

The court's judgment in this case indicates that the special investigative power for infiltration was applied for the entire operation, which may have enabled Dutch law enforcement officials to become a moderator and commit crimes (such as purchasing drugs). In the end, the officials were unable to climb the forum's hierarchical ladder to attain a moderator position.

However, Dutch law enforcement officials were able to contact a moderator of the online drug-trading forum. In doing so, they presumably used the special investigative power for systematic information gathering to interact with the suspect in an undercover capacity. A meeting was subsequently set up in the physical world to buy drugs. It is likely that the special investigative power for pseudo-purchase was applied for this part of the operation. After the drug transaction, the suspect was followed by an observation team, for which the special investigative power for systematic observation was applied. Dutch law enforcement authorities eventually successfully prosecuted five suspects for drug trading and arms trading.[84]

In this case, the judge noted how undercover investigative methods were applied in the physical world as well as 'virtually' under the application of the same special investigative power for infiltration. Despite the defendants' objections, the judges did not identify any problems with this 'hybrid' application of undercover investigative methods.[85] In my view, this hybrid application is indeed unproblematic, insofar as it is clear which investigative methods are authorised by which special investigative power and the relevant facts of the operation are disclosed to the suspects to provide sufficient transparency. Dutch law thus allows for both online and

83 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792.

84 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792.

85 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792. Siemerink (2000b, p. 144) considers this an aspect that will be common in online infiltration operations. Interactions with undercover agents can initially start online and then further develop in interactions in the physical world

offline application of this method. However, case law on online application is scarce. Therefore, while this single case sheds light on the online application of the special investigative power, the case law is insufficient for distinguishing a pattern as to how this digital investigative method is used in practice.

D Public guidelines

The Guideline for Special Investigative Powers offers much information about the use of infiltration as a special investigative power. Much of this information is already provided in legislative history. Therefore, only the most relevant information that helps to further clarify the scope of the investigative method and manner in which the investigative method is applied is presented below.

The guideline makes it clear that the special investigative power to infiltrate a criminal organisation allows law enforcement officials to use investigative methods that fall under the special investigative powers of systematic information gathering and pseudo-purchases. The authorisation of the special investigative power in question must mention the use of these other investigative methods as part of an infiltration operation. Infiltration operations should be executed by a special police team.[86]

Finally, the guideline further specifies the differences between the special investigative powers of infiltration and systematic information gathering. The first difference is that the special investigative power for infiltration authorises law enforcement officials to commit crimes that are in direct relation to the crimes of the criminal organisation,[87] which is not allowed when the special investigative power for systematic information gathering is applied. The second difference is that in infiltration operations, law enforcement officials participate in a criminal organisation, whereas during systematic information gathering they merely 'maintain contacts' with suspects or individuals involved in a criminal organisation. The third difference is that the special investigative power to infiltrate can only be applied with regard to a group of individuals that is preparing to commit or already committing crimes. This requirement does not apply to the special investigative power for systematic information gathering. The fourth difference is that the legal thresholds for using the special investigative power for systematic information gathering are lower than those for using the special investigative power for infiltration.

86 These police teams are specially trained. Further requirements for infiltration operations are specified in the 'Regeling infiltratieteams' (Regulation for infiltration teams) (*Stcrt.* 2001, no. 7), but they are not relevant to the research question at hand.

87 See also subsection 7.2.2 under D.

7.2.4 Section conclusion

With regard to online undercover methods, the foreseeability of the Dutch legal framework in criminal procedural law can be assessed based on the analyses conducted in subsections 7.2.1 to 7.2.3. The results of these analyses are summarised below.

The regulations for online pseudo-purchases in Dutch criminal procedural law are considered *foreseeable*. The reason is that statutory law clearly details that law enforcement officials can purchase goods or data using the special investigative power for pseudo-purchase. Dutch legislative history makes clear the investigative methods can be applied in an online context and there is a large amount of case law available that further indicates how the investigative method is applied in practice. Case law indicates that the special investigative power in art. 126i DCCP to conduct a(n) (online) pseudo-purchase is applicable as soon as law enforcement officials start the undercover operation and contact the suspect to buy the (illegal) good offered on an online trading platform. The Guideline for Special Investigative Power does not mention that the investigative method can be applied in an online context, but details the manner it is applied in the physical world. The manner the investigative method are applied in an online context and the physical world are similar and due to its one-time application limited in scope. Therefore, no specific regulations are in my view required for application of the investigative method in an online context.

The regulations for online interactions with individuals in Dutch criminal procedural law are considered *not foreseeable*. The special investigative power for systematic information gathering in the DCCP, which regulates the investigative method, only applies when the investigative method is applied systematically. However, the lack of guidance in the explanatory memoranda to the Special Investigative Powers Act and Computer Crime Act II, the lack of case law, and the lack of direction in the Guideline for Special Investigative Powers, means it remains unclear when the investigative method becomes systematic in nature and hence when the special investigative power for systematic information gathering must be applied. There are no factors provided by the legislator to determine when the investigative method is applied systematically, as opposed to the investigative method of observation. It is unclear whether the same factors are also suitable for the special investigative power of systematic information gathering. This creates ambiguity with regard to the scope of the investigative method and how the manner the investigative method is applied in Dutch law. It is important that the scope of the investigative method is detailed in statutory law or guidelines, because the text of the provision for systematic information gathering is very broad. It is currently unclear which online applications of the special investigative power are legitimate.

The regulations for online infiltration operations in Dutch criminal procedural are considered *foreseeable* in this study. The special investigative power for infiltration indicates the scope of the investigative method and the

requirements that must be met before the investigative method is applied. The prohibition of entrapment clearly restricts the scope of the investigative method and the manner the investigative method is applied. These detailed regulations for the investigative method are desirable, because the investigative method seriously interferes with the right to privacy of the individuals involved and the undercover interactions with poses risks with regard to entrapment in online infiltration operations. The privacy interference and risks of entrapment are in my view not greater in an online context. The explanatory memoranda to the Special Investigative Powers Act and Computer Crime Act II clearly state that the special investigative power can be applied in an online context. Case law concerning the online application of the investigative method is scarce, but also confirms the special investigative power can be applied in online context and indicates in which manner it may take place. Finally, the Guideline for Special Investigative Power indicates the scope of the investigative method in detail for its application on the physical world, but not in the digital world. The guideline does explain the difference of the special investigative power compared to the special investigative powers of systematic observation, pseudo-purchases, and systematic information gathering. The examined legal sources thus clarify (1) when the use of the special investigative power for infiltration is appropriate and (2) in which manner the investigative method can be applied.

7.3 Quality of the law

The normative requirement regarding the quality of the law, means that the ECtHR can specify the level of detail required for the description the investigative power and the minimum procedural safeguards that must be implemented vis-à-vis a particular method that interferes with the right to privacy. The detail that the ECtHR requires in the law and procedural safeguards depends on the gravity of the privacy interference that takes place.[88]

The desired quality of the law for online undercover investigative methods has been determined in Chapter 4, in subsection 4.3.3. As explained in the introduction of the chapter, the ECtHR has articulated qualitative requirements for the domestic legal frameworks of contracting States to prevent entrapment from occurring and to ensure a fair trial as protected by art. 6 ECHR. These requirements are such that it is possible to transpose them to requirements for the *regulation* of undercover operations. As such, these requirements are taken as a point of departure as the desirable quality of the law. The ECtHR has specified in case law that it requires *detailed regulations* to ensure transparency regarding an undercover operation and aim to prevent entrapment by law enforcement authorities. In addition, the ECtHR has repeatedly emphasised in case law that *supervision of an investigative judge* is

88 See subsection 3.2.2 under C.

'most appropriate' for undercover operations. Nevertheless, the ECtHR also accepts the supervision of a public prosecutor, insofar 'adequate procedures and safeguards' are available.[89] The desired quality of the law for undercover investigative methods is illustrated in Figure 7.2.

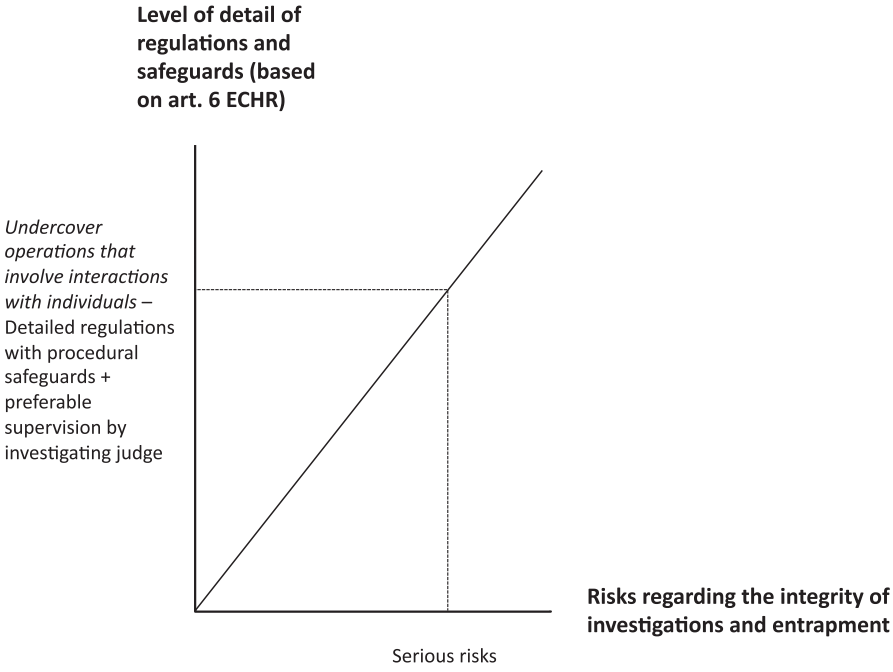

Figure 7.2: The desired quality of the law for undercover investigative methods.

Figure 7.2 illustrates how the scale of gravity looks different for undercover investigative methods than it does for the investigative methods examined in chapters 5 and 6. This difference is attributable to the fact that the ECtHR essentially requires a quality of the law for undercover methods, but does not differentiate between undercover variants. All investigative methods that involve undercover interactions with individuals in which serious risks of entrapment arise must have both detailed regulations that ensure transparency concerning the investigation and adequate supervision to prevent entrapment from taking place.

From a general point of view, the analysis in sections 7.1 and 7.2 has shown that Dutch law has detailed regulations for undercover investigative methods. These regulations are deemed desirable due to the privacy interference that accompanies these methods and the risks regarding the

89 See subsection 4.3.1.

integrity of the investigation.[90] The analysis in subsection 4.3.2 has shown that law enforcement officials can apply online investigative methods on a global scale and relatively anonymously, thanks to the characteristics of the Internet. However, in my view these characteristics generally do not significantly influence the gravity of the privacy interference or risks regarding the integrity of an investigation. The manner the investigative method is applied are the same; they only take place in a different context or with different communication services.

In the remainder of this section, the quality of the Dutch legal framework is tested with regard to each of the identified online undercover investigative methods. In subsections 7.3.1 to 7.3.3, the quality of the law of the special investigative powers that regulate the identified online undercover investigative methods is compared to the desired quality of the law. Subsection 7.3.4 presents conclusions regarding the adequacy of the quality of the Dutch legal framework for the digital investigative method.

7.3.1 Online pseudo-purchases

In the Netherlands, using pseudo-purchases as an investigative method is considered an undercover investigative method that requires detailed regulations in the DCCP.[91] The special investigative power that regulates pseudo-purchases can be applied only once in a criminal investigation with regard to crimes that are stipulated in art. 67(1) DCCP (including cybercrimes).[92] An order from a public prosecutor is required to apply the special investigative power. The involvement of a public prosecutor thus functions as a procedural safeguard to protect both the integrity of the investigation and the right to privacy of the individuals who are involved in it.[93] Public prosecutors must also apply the proportionality and subsidiary test to determine whether the application of the investigative method is legitimate. [94]

The undercover operation is restricted in time and scope since only authorises a single pseudo-purchase. As explained in subsection 4.3.2, I regard the privacy interference the application of the investigative method causes as serious, but not as serious compared to online undercover interactions (that can cover a broader set of operations and which operations can take longer in time) and online infiltrating operations (that involve the participation in crime and the possibility to commit crimes) as online undercover investigative methods.

---

90 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 3.

91 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 2, 23, and 33-34.

92 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 33.

93 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 3.

94 See also subsection 3.2.3.

The Dutch special investigative power for pseudo-purchase also specifically notes that law enforcement officials are not allowed to incite a suspect to commit a crime that this suspect did not intend to commit.[95] It thus explicitly prohibits entrapment by law enforcement officials. The risk of entrapment is also present in online pseudo-purchases, because law enforcement officials interact in an undercover capacity with suspect in order to purchase the good. These undercover law enforcement officials are thus not authorised to pressure a suspect to sell a good or data, which he did not intend to sell. The examined case law in subsection 7.2.1 indicates that the special investigative power that authorises an online pseudo-purchase was applied when illegal goods were already offered on online trading platforms. In that situation, the risk of entrapment appears small, since the suspect has a predisposition to commit the crime and it likely does not require effort to come to an agreement to purchase the good.

Subsection 4.3.3 identified the desirable quality of the law concerning pseudo-purchases to be detailed regulations and the involvement of a public prosecutor to supervise the application of the investigative method. Considering the above analysis, it can be concluded the Dutch regulations for pseudo-purchases *meet the desired quality of the law*, insofar the special investigative power to conduct a pseudo-purchase is applied.

7.3.2 Online undercover interactions with individuals

The analyses in subsections 7.1.2 and 7.2.2 have shown that the legal basis for online undercover interactions with individuals as an investigative method is derived from either (1) the description in art. 3 of the Dutch Police Act of the statutory duty of law enforcement officials to investigate crime or (2) the special investigative power for systematic information gathering. Based on the examined sources in law in subsection 7.2.2, it not clear exactly when the application of the investigative method becomes systematic in nature and hence when it is appropriate to apply the special investigative power.

The Dutch legislature considers the privacy interference that occurs when this investigative method is applied to be minor in nature, insofar as the method is not applied systematically. However, this argument fails to take the risk of entrapment and important role of supervision in these undercover investigations into account. For example, in the past Dutch law enforcement officials have attempted to pose as a minor in online chat rooms to gather evidence about individuals who want to engage in sexual activi-

95 See art. 126i(3) DCCP.

ties with minors in these online spaces and possibly in the physical world.[96] Smeets (2013, p. 335) implies that the legal basis that was used for the undercover operation was art. 3 of the Dutch Police Act and not the special investigative power of systematic information gathering. The judgement itself does not provide clarity on this issue.[97] Nevertheless, it is clear that law enforcement officials posed as a minor in a chat room to combat grooming. The risk of entrapment is considerable in this context, as the undercover investigative method requires law enforcement officials to actively engage with the individuals involved. To prevent entrapment from taking place, law enforcement officials will need to have a reasonable suspicion that a crime is taking (or will take) place and be able to prove a suspect's predisposition.[98] This investigative method is different from using *passive* decoys, such as unlocked bicycles that may lure bicycle thieves, which Dutch courts have previously found legitimate.[99] If the goal is to successfully prosecute a suspect for grooming by gathering evidence obtained while posing as a minor, the undercover agent must gain the individual's trust by interacting and having conversations of a sexual nature with him or her; the result may then be that the suspect proposes a meeting to engage in sexual activities. It may thus be challenging for law enforcement officials to remain 'essentially passive' in this kind of online undercover operation (cf. Smeets 2013, p. 336 and Ölçer 2014, p. 18). As explained in the introduction of section 7.3, the ECtHR desires detailed regulations and preferably the supervision of an investigative judge for the application of undercover investigative methods in which the risk of entrapment arises. In this case, the risk of entrapment is clearly present and a higher authority than law enforcement officials should test whether the undercover operation is legitimate considering the risk of entrapment. The ECtHR prefers that an investigative judge supervises the operation. In this case, the undercover operation was likely based on art. 3 of the Dutch Police Act, which does not require the authorisation of a public prosecutor. Even when the special investigative power of systematic gathering was applied in this case, it may have been more appropriate that an

96 See Jarl Van der Ploeg, 'Inzet 'lokpuber' komt weer in beeld', *Volkskrant*, 11 January 2014. Available at: http://www.volkskrant.nl/archief/inzet-lokpuber-komt-weer-in-beeld~a3575528/. When an actual meeting is arranged, the act may amount to the crime of grooming. Questions with regard to the use of a 'virtual child' to combat grooming are not addressed in this study. See Michelle Starr, 'First man convicted in child predator sting with virtual girl Sweetie', *CNET* 21 October 2014. Available at: http://www.cnet.com/news/first-man-convicted-in-child-predator-sting-with-virtual-girl-sweetie/ (last visited on 22 April 2015). See also the letter of 28 November 2013 to the Dutch Parliament from the Minister of Security and Justice concerning the news reports that 'a virtual Filipina girl traced 1000 child molesters'.

97 See Hof Den Haag, 25 June 2013, ECLI:NL:GHDHA:2013:2302.

98 Reasonable suspicion and a suspect's predisposition to the crime may be obtained after reports that indicate specific chat rooms in which relevant activities take place have been filed.

99 See HR 28 October 2008, ECLI:NL:HR:2008:BE9817, *VA* 2009, no. 1, m.nt. J. Silvis.

investigative judge supervises the investigation due to the intrusiveness of the investigative method and the high risk of entrapment.[100]

In my view, the Dutch legal framework for this investigative method does *not meet the desirable quality of the law*. At present, (online) undercover investigative methods can be based on either (1) the general legal basis in art. 3 of the Dutch Police Act or (2) the special investigative power for systematic information gathering, which is not even restricted to serious crimes. These regulations are not sufficiently detailed and do not provide the procedural safeguards needed to meet the desired quality of the law. A special investigative power that regulates (online) undercover interactions with individuals and requires authorisation from (or at least the involvement of) a public prosecutor is instead desirable (cf. Janssen 2015, p. 681-682).[101]

From a legal system viewpoint, it is also logical to have an investigative judge supervise undercover operations where entrapment is a risk. In the Netherlands, investigative judges have the responsibility to supervise the legitimacy of the application of investigative methods and ensure that the interests of (1) the investigation and (2) the suspect are balanced (cf. Corstens & Borgers 2014, p. 264). Since 2012, Dutch investigative judges have taken on a more coordinating function for evidence-gathering activities in criminal investigations.[102] As Corstens and Borgers (2014, p. 362) point out, law enforcement officials and public prosecutors are the 'natural adversaries' of suspects, while investigative judges are perceived as more independent in the Netherlands. Investigative judges can therefore serve an important function by safeguarding the integrity of a criminal investigation and preventing entrapment, both of which are particularly important in undercover investigations.

7.3.3 Online infiltration operations

The desirable quality of the law for online infiltration operations was formulated in subsection 4.3.3 as (1) a detailed legal basis in law for applying the investigative method and (2) the procedural safeguard of an investigative judge to supervise the online undercover investigative method. The involvement of an investigative judge is a desirable procedural safeguard, as infiltration operations involve considerable risks that endanger the integrity of criminal investigations.

---

100 See also *Rechtspraak.nl*, 'Advies Rechtspraak: Regel inzet van 'lokpuber' beter', 31 October 2014. Available at: http://www.rechtspraak.nl/Actualiteiten/Nieuws/Pages/Advies-Raad-regel-inzet-van-lokpuber-beter.aspx (last visited on 16 April 2015).

101 See also Ölçer 2015, p. 307, who argues that a warrant an of investigative judge should be considered by the Dutch legislature for the special investigative powers relating to undercover investigative methods. See also ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09 (*EHRC* 2015/1, m. nt. Ölçer at 9.

102 As a result of the Act on Strengthening the Position of the Investigative Judge (*Stb*. 2012, 408). See Parliamentary Series II 2009/10, 32 177, no. 2 (explanatory memorandum Act on Strengthening the Position of the Investigative Judge), p. 1.

In the Netherlands, stringent requirements must be fulfilled before the special investigative power for infiltration can be applied.[103] According to the Dutch legislature, these stringent conditions are necessary due to the risk that an operation will endanger a criminal investigation's integrity and the privacy interference that occurs when this investigative method is applied.[104] Apart from the DCCP, more detailed procedures are specified in public guidelines. In its legislation the Dutch legislature explicitly mentions how 'moral dilemmas' are present in undercover investigative methods, due to the fact that law enforcement officials (1) are authorised to commit crimes, (2) the risk they participate in unauthorised crimes, and (3) are subjected to safety risks.[105] Based on this legislative history, the Dutch legislature appears to be well aware of the risks involving infiltration operations and the danger of entrapment.[106] This is also reflected by the application of an extra procedural safeguard. Legislative history describes how – apart from the stringent requirements in the special investigative power itself – an operation must be consulted with a special commission of the Public Prosecution Service.[107] This commission will test (again) whether the operation is proportional in light of the relevant circumstances and determine if any other investigative methods that could be used to achieve the same result are available.

However, authorisation from an *investigative judge* is not required to apply the special investigative power for infiltration, and thus also for online infiltration operations. As a result, the current regulations for online infiltration in Dutch law do *not meet the desired quality of the law*. The Dutch legislature should consider adding a supervisory role for an investigative judge as an extra safeguard (cf. Janssen 2015). This extra safeguard is appropriate when the intrusiveness of the investigative method and the accompanying risks with regard to the integrity of the investigation are taken into account. An investigative judge can carefully balance the interests of both the investigation and the suspect.

7.3.4 Section conclusion

This section has compared the quality of the law of the current Dutch legal framework in criminal procedural law with the desirable quality of the law as determined in subsection 4.3.3. The results of the analyses conducted in subsections 7.3.1 to 7.3.3 are summarised below.

---

103 See subsections 7.1.3 and 7.2.3.

104 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29-30 and p. 34.

105 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29.

106 See, e.g., *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 31, p. 34, p. 74-75, and p. 120.

107 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 15.

The investigative method of online pseudo-purchases is regulated in detail in Dutch statutory law. The risk of entrapment is low when this investigative method is applied and the method does not interfere with the involved individuals' right to privacy in a particularly serious manner. For that reason, the detailed regulations for the investigative method and the required authorisation from a public prosecutor to use the special investigative power were found to *meet the desirable quality of the law*.

The Dutch legal framework for the investigative method of online undercover interactions with individuals *does not meet the desired quality of the law*. The first reason for this assessment is that the investigative method is not regulated in a foreseeable manner in the Dutch legal framework, due to ambiguity with regard to the question when the investigative method is applied in a systematic manner. The analysis again shows that the normative requirements of foreseeability and the quality of the law are intertwined. The second reason is that the analysis in section 4.3 showed that supervision from an investigative judge is desirable when there is a risk of entrapment in the application of this method. The special investigative power that is currently applicable when the investigative method is applied systematically only requires authorisation from a public prosecutor, not mandatory supervision from an investigative judge.

The investigative method of online infiltration operations with individuals does *not meet the desired quality of the law*. The reason is that the analysis in section 4.3 indicated that authorisation from an investigative judge is appropriate for the investigative method. This procedural safeguard is not required in the special investigative power for infiltration. In the Netherlands, only the authorisation of a public prosecutor is required.

7.4 Improving the legal framework

This section discusses how the DCCP can be improved to provide an adequate legal framework for regulating online undercover investigative methods. A legal framework is considered adequate when (1) it is accessible, (2) it is foreseeable, and (3) the desired quality of the law in the sense of procedural safeguards is met. The results of the analyses of the three normative requirements (as presented in sections 7.1 to 7.3) are summarised in Table 7.1.

Normative requirement	**Online pseudo-purchases**	**Online undercover interactions**	**Online infiltration operations**
Accessible	✓	✓	✓
Foreseeable	✓	✗	✓
Meets the desirable quality of the law	✓	✗	✗

Table 7.1: Representation of the research results in sections 7.1 to 7.3 (✓ = adequate, ✗ = not adequate).

This overview of the research results from sections 7.1 to 7.3 shows that the detailed regulations for undercover investigative methods have created an accessible legal framework. The Dutch legislature was quick to point out that the special investigative powers for undercover investigative methods can also be applied on the Internet. However, this statement alone does not create a foreseeable legal framework; further guidance and elaboration is necessary for certain online undercover investigative methods.

According to the Dutch legislature, the Dutch legal framework for special investigative powers only requires amendments when *"the specific nature of investigations in a computerised environment"* merits specific legislation.[108] This chapter has shown that it is not the change of environment that necessitates amendments to the legal framework for online undercover investigative methods, but the heightened procedural safeguards (preferably an investigative judge) for the regulation of the investigative methods that are derived from ECtHR case law. The online application of undercover investigative methods is not more privacy intrusive, since the investigative technique that is used are the same and bring with similar privacy interferences. The online application also does not create more risks regarding the integrity of an investigation than offline variants, although the risk of entrapment remains present.

Improvements to the Dutch legal framework are proposed for each of the identified online undercover investigative methods in subsections 7.4.1 to 7.4.3.

7.4.1 Online pseudo-purchases

The Dutch legal framework for online pseudo-purchases is deemed to be accessible and foreseeable and to offer a sufficient quality of the law. The Dutch Ministry of Security and Justice has recommended that the requirement that data is 'stored, processed or transferred by an automated device through the intermediary of public telecommunication network' in the special investigative power to conduct a pseudo-purchase in art. 126i(1)(b) DCCP be removed. The reason for this proposal is that data can also be transferred by other means of communication; the special investigative power should simply indicate that law enforcement officials can buy data from a suspect as part of a pseudo-purchase.[109] I agree with the suggestion to remove this redundant text from the special investigative power for pseudo-purchases (*Recommendation I*).

108 *Kamerstukken II* (Parliamentary Series Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum to the Computer Crime Act II), p. 36.

109 See the discussion document regarding special investigative powers (6 June 2014), p. 30.

7.4.2 Online undercover interactions with individuals

The legal basis in Dutch criminal procedural law for using online undercover interactions with individuals as an investigative method is currently too ambiguous. It is not clear when undercover interactions with individuals are deemed 'systematic in nature' and hence when the special investigative power for systematic information gathering must be applied. The regulations for this investigative method can be improved as follows.

First, the foreseeability of the method can be strengthened by requiring the application of the special investigative power for systematic information gathering whenever law enforcement officials launch undercover operations that involve undercover interactions with individuals as opposed to only requiring the special investigative power when the investigative method is conducted in a systematic manner (*Recommendation 2*). At the start of such an operation, officials must indicate in which manner they intend to interact with an individual and how much time they think they will require to gather sufficient evidence for their criminal investigation. The text of the special investigative power itself can be improved by stating more clearly that law enforcement officials can gather the information by interacting with the suspect and his direct environment (both offline and online).[110]

Second, to improve the quality of the law, it is desirable to involve an investigative judge to supervise the undercover operation. The prohibition of entrapment should also apply in the context of the special investigative power for (systematic) information gathering (*Recommendation 3*). In that respect, it is noteworthy that the Dutch Minister of Security and Justice proposed to mention the prohibition of entrapment explicitly in the general provisions for pre-trial investigations of the DCCP.[111] The provision will make it explicit that the prohibition of entrapment applies to all investigative methods.

Third, more stringent legal thresholds are desirable for the application of the method, considering the high intrusiveness of the special investigative power. Undercover law enforcement officials can gain intimate knowledge about the private lives of the individuals involved – also individuals in the direct environment of the suspect – when the investigative method is applied (both in an online and offline context). On that basis, the application of the special investigative power should be restricted to criminal investigations involving more serious crimes, as defined in art. 67 DCCP (*Recommendation 4*).[112]

---

110 See also the discussion document regarding special investigative powers (6 June 2014), p. 28.

111 See the discussion document regarding the general provisions for pre-trial investigations (6 June 2014), p. 20.

112 See also p. 26 of the discussion document regarding the special investigative powers of 2014 as part of the modernisation programme for Dutch criminal procedural law, which contains a suggestion to increase the special investigative power for criminal investigations with a minimum prison sentence of one year or more.

7.4.3 Online infiltration operations

The use of an infiltration operation as an investigative method is regulated in detail in Dutch criminal procedural law. The special investigative power for infiltration must also be used for online infiltration operations. The Dutch legal framework for online infiltration operations can be considered as accessible and foreseeable, due to the detailed regulations that specify the scope of the investigative method and the manner in which the method can be applied. The additional safeguard of a mandatory review by the special commission of the Dutch Public Prosecution Service is applicable to infiltration operations.

However, the supervision of an investigative judge in undercover operations, which is preferred by the ECtHR, is notably absent in Dutch criminal procedural law for infiltration operations. The mandatory involvement of an investigative judge is thus recommended for the application of the special investigative power for infiltration (*Recommendation 5*).

7.5 Chapter conclusion

The aim of this chapter was to determine how Dutch criminal procedural law should be improved to adequately regulate online undercover investigative methods (RQ 4c). To answer the research question, the Dutch legal framework regulating online undercover investigative methods (i.e., online pseudo-purchases, online undercover interactions with individuals, and online infiltration operations) was investigated with regard to (1) its accessibility, (2) its foreseeability, and (3) the desired quality of the law.

From a broad perspective, Dutch criminal procedural law provides a solid legal basis for investigative methods by outlining detailed corresponding regulations. The Dutch legislature has also been visionary by stating as early as in 1997 that undercover investigative methods can also be applied in an online context. However, statements alone do not create a foreseeable legal basis for those investigative methods that are regulated by special investigative powers with a broad description, most notably with regard to the special investigative power for systematic information gathering.

The results of the adequacy of the Dutch regulation for the investigative method in terms of the three normative requirements are summarised in subsection 7.5.1. The specific recommendations that arise from these results are presented in subsection 7.5.2.

7.5.1 Summary of conclusions

Section 7.1 analysed the accessibility of the Dutch legal framework for online undercover investigative methods. In the Netherlands, detailed regulations for undercover investigative methods are created in the DCCP. The Dutch legislature already stated in 1997 that the special investigative powers that

regulate undercover investigative methods are also applicable in the context of the Internet. An indication of the applicable regulations for the investigative methods is thus provided in the Dutch law. As a result, the Dutch legal framework for online undercover investigative methods should be regarded as accessible.

In section 7.2, the analysis of the foreseeability of online undercover investigative methods showed that (1) the scope of the investigative method of online pseudo-purchases and (2) the manner in which Dutch law enforcement authorities exercise the investigative power for pseudo-purchases are clear. The legal basis in Dutch criminal procedural law for applying the investigative method of online undercover interactions with individuals is not sufficiently clear. Online undercover interactions require the application of a special investigative power once the investigative method is applied 'systematically'. However, due to a lack of guidance in (1) statutory law, (2) the explanatory memoranda of the Special Investigative Powers Act and the Computer Crime Act II, (3) case law, and (4) the Guideline for Special Investigative Powers, it is unclear at what point the application of this method becomes systematic. Finally, online infiltration operations are regulated in detail by the special investigation order for infiltration in Dutch criminal procedural law. The examined legal sources indicate with sufficient clarity the (1) scope of the investigative method and (2) the manner in which the method is applied.

The analysis of the desired quality of the law conducted in section 7.3 showed that the Dutch legal framework does not meet the desired quality of the law for all three online undercover investigative methods. The detailed regulations for online pseudo-purchases, which include mandatory authorisation from a public prosecutor and restriction to serious crimes, are deemed to be of sufficient quality. When this digital investigative method is applied, risks related to both entrapment and the integrity of the investigation appear lower than for the other two digital investigative methods. With regard to the regulations for (1) online undercover interactions with individuals involved in criminal investigations and (2) online infiltration operations, the preferable involvement of an investigative judge is notably absent. Both investigative methods seriously interfere with the involved individuals' right to privacy and generate risks related to the integrity of criminal investigations. Furthermore, based on the desired quality of the law that has been derived from art. 6 ECHR, the involvement of an investigative judge is appropriate for all undercover investigative methods that entail a higher risk of entrapment. The involvement of an investigative judge in these investigative methods is therefore merited.

7.5.2 Recommendations

Section 7.4 presented five recommendations to improve the Dutch legal framework for online undercover investigative methods. These recommendations followed the analysis of the adequacy of the Dutch legal framework

based on the three normative requirements in sections 7.1 to 7.3. These recommendations are as follows.

1. The special investigative power to conduct a pseudo-purchase should be amended by removing the redundant text stating that data can be purchased that is 'stored or transferred by an automated device through the intermediary of public telecommunication network'.
2. The Dutch legislature should create a more foreseeable legal basis for the application of the investigative method of undercover online interactions with individuals. A special investigative power should regulate the use of this investigative method that indicates more clearly that it involves undercover interactions with suspects or individuals in their direct environment.
3. The Dutch legislature should improve the quality of the law for the special investigative power for systematic information gathering by requiring the supervision of an investigative judge. This improvement is suggested considering the risks related to undercover operations, which include the serious risk of entrapment and risks regarding the integrity of criminal investigations. The prohibition of entrapment should also apply to the special investigative power for systematic information gathering.
4. The Dutch legislature should also improve the special investigative power for systematic information gathering by restricting the application of this special investigative power to criminal investigations involving the more serious crimes defined in art. 67 DCCP. This improvement is suggested considering the seriousness of the privacy interference that accompanies the application of this undercover investigative method.
5. The Dutch legislature should require the involvement of an investigative judge to supervise online infiltration operations that necessitate the application of the special investigative power for infiltration. This improvement is suggested considering the risks related to undercover operations, which include the serious risk of entrapment and risks regarding the integrity of criminal investigations.

8 Performing hacking as an investigative method

This chapter aims to answer the fourth research question with regard to hacking as an investigative method (RQ 4d): *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate hacking as an investigative method?* Hacking as an investigative method is distinguished in this study as: (1) network searches, (2) remote searches, and (3) the use of policeware.

To answer this research question, the investigative method is placed within the Dutch legal framework and further analysed to determine whether the normative requirements for regulating investigative methods which flow forth from art. 8 ECHR are fulfilled. In chapter 3, the normative requirements were identified as follows: (1) accessibility, (2) foreseeability, and (3) the quality of the law.

The requirements for the regulation of this investigative method on the basis of art. 8 ECHR were formulated in subsection 4.4.3. The investigative method was compared to a computer search, i.e., a search at a place where computers (not connected to other computers or the Internet) are seized and their contents are analysed. Computer searches are themselves very intrusive investigative methods that merit detailed regulations with strong procedural safeguards, preferably a warrant from an investigative judge. Network searches are similar, but they go a step further, as this investigative method enables law enforcement officials to search computers elsewhere that are connected to a seized computer. Remote searches and the use of policeware are clearly more privacy intrusive than computer and network searches, given that they are applied covertly. In contrast, a network search is conducted during a search in the physical world. The suspect will be aware of the application of network search, but not necessarily which computers are remotely accessed. The suspect will likely not detect law enforcement officials when a remote search is conducted or policeware is used. As covert applications of investigative methods are accompanied by higher risks of abuse by law enforcement authorities, they merit strong procedural safeguards. Here again, a warrant from an investigative judge is desirable. The use of policeware should also be regulated in detail with added procedural safeguards in the form of restrictions concerning the duration and functionalities of policeware. With regards to hacking as an investigative method, the point of departure here is again that the requirements that flow forth from art. 8 ECHR are minimum standards and that Dutch criminal procedural law can impose a higher level of protection than art. 8 ECHR offers to the individuals involved.

Brief description of the applicable legal framework
Dutch criminal procedural law currently does not include any special investigative power that distinctly regulates the investigative power for remotely accessing computer systems after which a remote search can be conducted or policeware can be installed on the accessed computer (cf. Oerlemans 2011, p. 901-903). A special investigative power is available for network searches, which is examined extensively in sections 8.1.1 and 8.2.1. As explained in section 4.4, the investigative methods of remote searches and use of policeware are highly privacy intrusive. As explained in the introduction to chapter 5, as part of its regulation of investigative methods, Dutch law requires that investigative methods that interfere with the involved individuals' rights and freedoms in more than a minor manner or threaten the integrity of the criminal investigation are based in specific provisions in Dutch criminal procedural law. In December 2015, the Computer Crime Act III was published. This bill aims to explicitly regulate remote searches, the use of policeware, and other forms of hacking as an investigative method (but not network searches), as a special investigative power.

However, it can also be argued that the types of hacking identified as investigative methods within this study can be based on existing investigative powers (cf. Boek 2000 and Verbeek, de Roos & van den Herik 2000). These are the regulations for traditional searches (during which computers can be seized), sneak-and-peak operations, and the use of covert listening devices.[1] In Figure 8.1, these investigative methods are placed on the scale of gravity for privacy interferences with the accompanying quality of the law in the Dutch legal framework.

1 These investigative methods are considered extensively in sections 8.1 and 8.2.

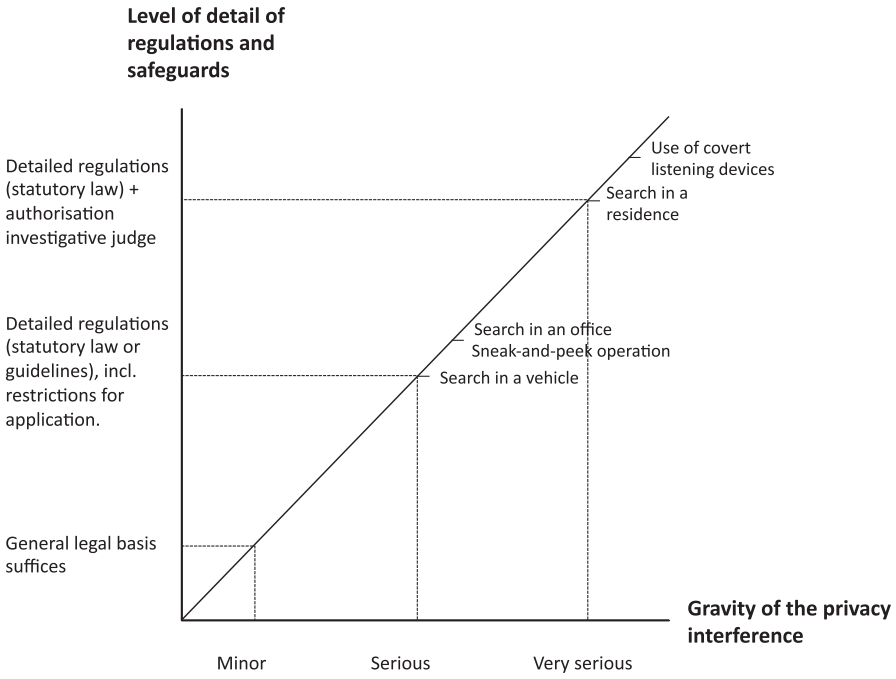

Figure 8.1: The Dutch scale of gravity for investigative methods that are mentioned as a possible legal basis for hacking as an investigative method.

Figure 8.1 illustrates how Dutch law regulates the above-mentioned investigative methods in detail and how different procedural safeguards are required when applying each method (which depend on the gravity of the investigative method)

This chapter further examines whether the identified types of hacking, that can be applied anywhere, can indeed be based on the existing provisions regulating the investigative methods mentioned above. If so, it is examined whether any amendments are required to these provisions to accommodate the identified types of hacking as an investigative method. If not, it is examined whether new distinct legal basis altogether are required for the three types of hacking.

The Dutch legal framework for hacking as an investigative method should fulfil the normative requirements of (1) being accessible, (2) being foreseeable, and (3) meeting the quality of the law that has been derived from art. 8 ECHR. The proposed special investigative power to regulate hacking as an investigative method is also considered in section 8.4. Section 8.4 specifically addresses the question how the Dutch legal framework can be improved to adequately regulate hacking as an investigative method.

Structure of the chapter
The structure of the chapter is as follows. In each section, all three types of hacking as an investigative method are discussed. To assess the accessibility and foreseeability of the Dutch legal framework with regard to the investigative methods, the same scheme of research is used as in chapters 5, 6 and 7. That research scheme consists of the examination of the following four sources of law: (A) statutory law, (B) legislative history, (C) case law, and (D) public guidelines. Thereafter, the requirements for regulations extracted from art. 8 ECHR in chapter 4 are compared to the Dutch legal framework. Based on the results of the analyses, recommendations to improve the Dutch legal framework are provided.

Thus, in section 8.1, the *accessibility* of the regulations for hacking as an investigative method in the Dutch legal framework is examined. Section 8.2 analyses to which extent hacking as an investigative method is regulated in a *foreseeable* manner in the Netherlands. Section 8.3 examines whether the Dutch legal framework for hacking as an investigative method meets the *desired quality of the law*. Based on the findings of section 8.1 to 8.3, section 8.4 will provide concrete suggestions on how Dutch criminal procedural law can be improved to adequately regulate hacking as an investigative method. Section 8.5 concludes the chapter with a summary of findings.

8.1 Accessibility

An accessible basis in law means that the law gives an adequate indication concerning the regulations for the use of investigative methods in a given case.[2] The examination of this normative requirement in relation to hacking as an investigative method will be conducted via analysis of the existing regulations of investigative methods, which may already serve as a legal basis for the digital investigative methods.[3] Subsections 8.1.1 to 8.1.3 present the analyses for all three types of hacking considered. Subsection 8.1.4 then provides conclusions regarding the accessibility of this investigative method in Dutch law.

8.1.1 Network searches

A network search is an investigative method that is used during a search at a particular place (in the physical world). For instance, law enforcement officials can seize a computer during a residence search. As part of a network search, law enforcement officials can then for instance examine an external hard drive or media player by accessing those devices from the previously seized computer through the (internal) network.

2 See subsection 3.2.2 under A.

3 This study does not examine the specific regulations for analysing privileged information, such as information from lawyers, physicians, and journalists.

Law enforcement officials can potentially also gain access to online services that an individual uses when they seize a running computer of the suspect (cf. Conings & Oerlemans 2013).[4] The prevalence of smartphone 'apps' with accompanying login credentials enable law enforcement officials to acquire login credentials when they seize computers (including smartphones). From that seized computer, and using these login credentials, law enforcement officials can access the same internet services that a suspect utilises.[5] A network search is also considered as a type of hacking as an investigative method, because law enforcement officials also gain remote access to computer systems, of which the suspect is not necessarily aware, when a network search is performed.

The accessibility of the legal basis for utilising a network search as an investigative method is examined below using the research scheme mentioned in the introduction to this chapter.

A Statutory law

Dutch criminal procedural law contains detailed regulations for the investigative method of a network search. The special investigative power in art. 125j(1) DCCP that regulates network searches reads as follows:

"In the event of a search, the data stored in a computer that is located elsewhere can be examined from the location that the search takes place, insofar this is reasonably required to uncover the truth. Data that is found, can be secured".[6]

The text of the special investigative power thus states that law enforcement officials can 'investigate data stored on a computer that is located elsewhere' during a search at a specific place (cf. Koops et al. 2012b, p. 59). It is emphasised here that the investigative method is conducted from a computer that has been previously seized by law enforcement authorities. For that reason, the investigative power refers back to the investigative powers for searching a place.

In order words, statutory law authorises law enforcement officials to gain remote access to an interconnected computer when they are conducting a search at a particular place. In the Netherlands, searches by law enforcement officials are regulated in detail in criminal procedural law. Different regulations and accompanying procedures and conditions may apply depending on where a search occurs, given that searches are more intrusive

4 See the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53, in which the Dutch Ministry of Security and Justice indicates that Dutch law enforcement officials can log in to a server of Gmail or Dropbox to access e-mails and documents stored in the cloud.

5 See subsection 2.4.3.

6 The special investigative power also indicates that the investigation cannot go further than those parts of a computer that the people who reside or work at the place where the search is conducted are authorised to access (see art. 125j(2) DCCP).

when they take place in certain locations. In the event of a criminal investigation related to the more serious crimes as defined in art. 67 DCCP, law enforcement officials can perform network searches on computers located:

(1) in a vehicle;
(2) any other place (except for residences or the offices of privileged professions), after acquiring authorisation from a public prosecutor; and
(3) at a residence, after acquiring authorisation from both a public prosecutor and an investigative judge (cf. Conings & Oerlemans 2013, p. 24).[7]

These three investigative powers were placed on a scale of gravity in Figure 8.1 in the introduction to this chapter. This figure illustrates that searches in vehicles are not considered as highly privacy intrusive and that law enforcement officials are not required to obtain authorisation from a higher authority, whereas residence searches are considered very privacy intrusive and require the procedural safeguard of a warrant from an investigative judge.

B Legislative history

The investigative power for a network search was first introduced by the Dutch legislature in 1992.[8] The legislature made it clear that during a search of a residence, law enforcement officials can seize devices on which data is stored and subsequently search that data.[9] It also found it necessary to create the special investigative power to search stored data on interconnected computers, since residence searches only authorise the search and seizure of computers located at a specific place.[10] Network searches enable data to be located on interconnected computers that are physically in different places.

From 1993-2005, law enforcement officials were only allowed to apply the investigative power to interconnecting computers when they were conducting a search at a residence. In 2005, the DCCP was amended to allow these officials to conduct network searches when they apply the investigative power to conduct a search in any (physical) place.[11]

7 In these three cases, the legal bases in Dutch criminal procedural law for conducting these investigative powers are respectively (1) art. 125j jo art. 96b DCCP, (2) art. 125j jo art. 96c DCCP, and (3) art. 125j jo art. 110 or 97 DCCP.

8 27 December 1992, *Stb.* 1993, 33.

9 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (Explanatory memorandum Computer Crime Act I), p. 11.

10 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (Explanatory memorandum Computer Crime Act I), p. 11-12. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 11.

11 *Stb.* 2005, 390. See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 19.

C Case law

Only *one* case that explicitly refers to the legal basis of a network search is available.[12] The Appeals Court of Amsterdam noted that that law enforcement officials can seize a computer in order to subsequently search that computer's stored contents. The special investigative power for conducting a search that is solely focused on retrieving data that is stored on computers (regulated in art. 125i DCCP) is applicable in this situation. The appeals court also noted that law enforcement officials can use the *"so-called network search"* (as specified in art. 125j DCCP).[13] The case did not provide any further information about how the investigative power for a network search is applied. With regard to the accessibility of the legal basis, it is clear that case law (also) provides an indication of the legal basis for the investigative method.

D Public guidelines

The Guideline for Special Investigative Powers, the Guideline for Child Pornography Investigations[14] and the Guideline for the Seizure of Objects[15] of the Public Prosecutors Service, do not mention the use of the special investigative power for network searches to gather evidence in a criminal investigation. The Guidelines for Child Pornography Investigations and the Seizure of Objects solely mention the possibility to seize computers during a search, after which the data stored on those computers may be examined for evidence-gathering purposes.[16] The Guideline for the Seizure of Objects only specifies the legal basis for the seizure of computers in detail in its Appendix I.[17] Thus, none of the guidelines indicates the legal basis for network searches.

8.1.2 Remote searches

The investigative method of a remote search refers to an evidence-gathering activity in which law enforcement officials remotely access a computer (through hacking) and search the data that is stored on it (cf. Brenner 2012). Law enforcement officials can take screen shots of the remotely accessed computer, prepare a written record of the evidence-gathering activities, or even copy relevant data for evidence-gathering purposes (cf. Oerlemans

12 Hof Amsterdam, 24 February 2016, ECLI:NL:GHAMS:2016:579.
13 Hof Amsterdam, 24 February 2016, ECLI:NL:GHAMS:2016:579.
14 *Stcrt.* 2016, 19415.
15 *Stcrt.* 2014, 18598.
16 For child pornography investigations, the guideline recommends seizing all devices and examining their contents. The guideline notes that the data may reveal *"insights in the behaviour of the suspect with regard to child pornography. Contacts, networks of child pornography users or clues that the suspect has abused children may [also] be determined by examining the contents on seized computers"* (translated by the author).
17 Under section B9.

2011, p. 892).[18] This investigative method can enable law enforcement officials to overcome the challenges of anonymity and encryption. Remote searches can be a powerful technique to identify suspects by determining the location and contents stored on a computer, even when a suspect obfuscates his originating (public) IP address with anonymising techniques or services.[19] The investigative method can also enable law enforcement officials to gain access a computer before a suspect is able to encrypt stored information. Law enforcement officials can also remotely access an online account by gaining remote access to a server with acquired login credentials and then copying relevant data.[20]

The accessibility of the legal basis for performing remote searches as an investigative method is examined below using the announced research scheme.

A Statutory law

No specific distinct provisions for remote searches are available in Dutch criminal procedural law. Three options thus arise: (1) the investigative method can be applied under the statutory duty of law enforcement officials to investigate crimes (art. 3 of the Dutch Police Act), (2) the investigative method can be based on an existing special investigative power, or (3) there is currently no legal basis for this method under Dutch law.

With regard to the first option, it is not likely that the investigative method of a remote search can be based on art. 3 of the Dutch Police Act. As explained in subsection 4.4.2, remote searches seriously interfere with the right to privacy as defined in art. 8 ECHR. As such, both ECtHR case law and the Dutch criminal procedural legality principle require that this investigative method be regulated in a specific provision in de DCCP. It is thus appropriate to regulate the investigative method as a special investigative power with adequate procedural safeguards (cf. Oerlemans 2011, p. 901).

With regard to the second option, only one author has argued that certain forms of hacking as an investigative method can be applied on an existing legal basis. Boek argued in 2000 that a remote search of a suspect's webmail account can be regarded as the digital equivalent of a 'sneak-and-peek operation'[21] (Boek 2000, p. 592).[22] Art. 126k DCCP regulates sneak-and-peek operations. The relevant provision reads as follows:

18 It should be noted that this application of a remote search also requires the use of policeware.
19 See subsection 2.3.3.
20 See subsection 2.4.3.
21 In Dutch: '*inkijkoperatie*'.
22 See art. 126k DCCP.

"In case of reasonable suspicion of a crime as defined in art. 67(1) DCCP and insofar it is in the interest of the investigation, a public prosecutor can order a law enforcement official to enter a private place without permission of the right holder, insofar it is not a residence, or to utilise a technical device to:

a. record the place;
b. secure evidence, or;
c. place a technical device in order to determine the presence or movements of an object."[23]

When law enforcement officials perform a sneak-and-peak operation in the physical world, they often slide a flexible camera under a doorpost to briefly observe a private place. In the explanatory memorandum to the Special Investigative Powers Act, the Dutch legislature described a 'private place' as a physical place, such as an office space or a garage. It also made it clear that a sneak-and-peek operation in a residence is considered a disproportionate investigative method for which no basis has been created in criminal procedural law.[24] A sneak-and-peek operation in a residence is thus not permissible. Boek argued that a 'hard disk' could also be regarded as a private place and thus that a sneak-and-peek operation could take place by hacking a computer (Boek 2000, p. 592).

However, I agree with Schermer (2003, p. 53), who regards viewing a computer as a private place in the context of a sneak-and-peek operation as a too extensive interpretation of art. 126k DCCP. I believe that the legislature clearly did not have the hacking of online accounts in mind when it created the investigative power for a sneak-and-peek operation (cf. Oerlemans 2011, p. 901-902). Remote searches interfere with the right to privacy in an entirely different manner than when a sneak-and-peek operation is applied. Furthermore, a remote search can also take place in a computer located at a residence. In contrast, art. 126k(1) DCCP explicitly excludes the possibility to conduct a sneak-and-peek operation inside a residence. The extensive interpretation of investigative powers to suit the needs of law enforcement authorities is not permitted and conflicts both with art. 8 ECHR and with the Dutch criminal procedural legality principle.

In 2002, the Dutch legislature explicitly created hacking powers for Dutch national security and intelligence services.[25] The Dutch legislator did not mention its intent to create such powers for criminal law enforcement authorities. As Koops and Buruma (2007, p. 118 in: Koops 2007) rightfully point out, legislative history thus strongly suggests that hacking powers (such as the possibility to conduct remote searches) have not been created for law enforcement authorities.

23 Translated by the author.
24 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 40, 43 and 70.
25 See art. 24 of the Intelligence and Security Services Act of 2002, *Stb.* 2002, 148.

In conclusion, option 3 mentioned above – that the Dutch legislature did not intend to provide Dutch law enforcement authorities with the power to hack computers – is most appropriate.

B Legislative history

Dutch legislative history does not indicate which legal basis is appropriate for a remote search. This investigative method is not mentioned in the explanatory memoranda to the Special Investigative Powers Act or both Computer Crime Acts.

C Case law

Only *one* judgment that deals with the legitimacy of the legal basis for conducting a remote search is available. This case has already been extensively considered in subsections 2.5.4 and 6.1.4.[26] The judgement of the Court of Rotterdam involves the remote access of a webmail account by a Dutch law enforcement official after acquiring authorisation from a public prosecutor. The legal basis for this operation is not made clear in the judgment. The public prosecutor deemed the remote search necessary to determine where a shipment of cocaine was delivered. The public prosecutor did not want to wait for the results of a mutual legal assistance request to acquire the contents of the webmail account using a data production order as meant in art. 126ng(2) DCCP, presumably as doing so would have created an unacceptable delay in the investigation. After remote access to the webmail account was obtained using login credentials previously acquired from an informant, information in e-mails revealed the location of the cocaine shipment (i.e., the port of Rotterdam).

In the first instance of the case, the judges noted that the data should have been obtained through a data production order instead of remotely accessing the online account.[27]

In second instance of the case, the judges did not comment on the legal basis for applying the investigative method. They instead simply stated that the webmail account did not belong (exclusively) to the suspect. For that reason, the suspect was not 'directly infringed in his interests' and no sanction was provided to the supposed procedural default.[28]

Taking the above facts of the case into account, the corresponding judgement ultimately does not provide an indication of the legal basis for gaining remote access to online accounts (technically to a server of the company that provides the webmail service).

---

26 See Rb. Rotterdam, 26 March 2010, ECLI:NL:RBROT:2010:BM2520 and Hof Den Haag, 27 April 2011, ECLI:NL:GHSGR:2011:BR6836.

27 Rb. Rotterdam, 26 March 2010, ECLI:NL:RBROT:2010:BM2520.

28 See Hof Den Haag, 27 April 2011, ECLI:NL:GHSGR:2011:BR6836. See further Oerlemans 2011, p. 894-896. That procedural default was not sanctioned can be explained by the Dutch '*Schutznorm*'. The concept of sanctioning procedural defaults is related to the right to fair trial in art. 6 ECHR. As this study is restricted to art. 8 ECHR, this concept is not further examined.

Indications of hacking as an investigative method in the media

Several news articles in the media and press releases issued by the Dutch Public Prosecution Service indicate that Dutch law enforcement officials have used remote searches as an investigative method at least four times.[29] Two cases are further examined below to analyse the legal basis that was used to conduct these operations.

In 2010, Dutch law enforcement authorities 'took over' the Bredolab botnet. As explained in subsection 2.1.1, a botnet is a network of infected computers (in this case infected by Bredolab malware) that can be controlled by a person (in this case, the suspect). The IT infrastructure of the botnet was located at a Dutch hosting provider. The infrastructure was complex and consisted of several VPN servers and proxy services in an attempt to obtain more anonymity by obscuring the IP address and several command-and-control servers. This convenient location and the cooperation of the hosting provider enabled Dutch law enforcement authorities to conduct a search at the hosting provider and 'take over' the infrastructure of the botnet (once they had hacked several servers and gained remote access to the botnet's command-and-control servers). Dutch law enforcement authorities located the suspect and sent a warning to computer users infected by the Bredolab malware, urging them to clean their computers and report the crime.[30] The suspect was located in Armenia and successfully prosecuted by that State.[31]

In 2011, Dutch law enforcement authorities obtained remote access to four Tor hidden services that were hosting child pornography. As explained in subsection 2.3.2, Tor not only permits individuals to use the Internet more anonymously; it also enables them to access services that are only accessible through Tor, which are called Tor hidden services. Websites or online forums that are only available via Tor sometimes offer child pornography materials to Tor users. In this criminal investigation, Dutch law enforcement officials

29 See Landelijk Parket, 'Dutch National Crime Squad announces takedown of dangerous botnet', 25 October 2010. Available at: https://www.om.nl/actueel/nieuwsberichten/@28332/dutch-national-crime/, Landelijk Parket, 'Kinderporno op anonieme, diep verborgen websites', 31 August 2011. Available at: http://www.om.nl/onderwerpen/zeden-kinderporno/@156657/kinderporno-anonieme/, Joost Schellevis, 'OM: politie brak in op router vanwege 'acute dreiging'', *Tweakers*, 6 November 2014. Available at: http://tweakers.net/nieuws/92427/om-politie-brak-in-op-router-vanwege-acute-dreiging.html, and see Landelijk Parket, 'Wereldwijde actie politie en justitie tegen hackers'. Available at: https://www.om.nl/vaste-onderdelen/zoeken/@85963/wereldwijde-actie (last visited on 21 December 2014).

30 See Landelijk Parket, 'Dutch National Crime Squad announces takedown of dangerous botnet', 25 October 2010. Available at: https://www.om.nl/actueel/nieuwsberichten/@28332/dutch-national-crime/ (last visited on 21 December 2014). Regarding the more technical details of the operation, see De Graaf, Shosha, and Gladyshev 2012. For a legal analysis of the case, see most notably Koning 2012.

31 See also Josh Halliday, 'Suspected Bredolab worm mastermind arrested in Armenia', *The Guardian*, 26 October 2012. Available at: https://www.theguardian.com/technology/2010/oct/26/bredolab-worm-suspect-arrested-armenia (last visited on 13 November 2015).

gained remote access to the webservers of these websites by hacking. They then replaced 220,000 pornographic images of children with the logo of the Dutch police. They also posted the following message on these websites warning Tor-users as follows: *"This site is under criminal investigation, by the Dutch National Police, you are not anonymous, we know who you are"*. It is not clear whether any suspects were prosecuted following the operation.[32]

These cybercrime investigations that utilised hacking as an investigative method led to the Dutch parliament posing questions to the Dutch Minister of Security and Justice in 2014. In his letter of response, the minister stated that Dutch law enforcement authorities had indeed obtained 'remote access to computers' in several criminal investigations.[33] He noted that in these special circumstances, the investigative power 'to search a place in order to secure data stored on a data carrier' (as articulated in art. 125i DCCP), grants Dutch law enforcement officials with the authority to gain remote computer access. Art. 125i DCCP, reads as follows:

"The investigative judge, the public prosecutor, the deputy public prosecutor and the investigating law enforcement officials are authorised – under the same conditions as provided in articles 96b, 96c(1)(2)(3), 97(1)(2)(3)(4), and 110(1)(2) – to search a place in order to secure data located at this place that is stored or recorded on a data carrier. This data can be secured in the interest of the investigation. (…)" [34]

Art. 125i DCCP thus authorises the appropriate authorities to secure data that is stored on computers under the existing legal basis to search a place. As these legal bases are already examined under A in subsection 8.1.1, it is not further considered here. The regulations for these searches are also illustrated in Figure 8.1 in the introduction. This author was able to review the dossier files of the Bredolab and Tor investigations and confirm that the special investigative power to search a place and secure data that is stored on computer was indeed utilised as a legal basis.[35] In both cases, Dutch law enforcement authorities obtained a warrant from an investigative judge to conduct the operation, although the legal basis that was used (art. 96c DCCP) does not require such a warrant.

---

32 See Landelijk Parket, 'Kinderporno op anonieme, diep verborgen websites', 31 August 2011. Available at: http://www.om.nl/onderwerpen/zeden-kinderporno/@156657/kinderporno-anonieme/. See also Wil Thijssen, 'De digitale onderwereld', *Volkskrant* 10 March 2012. Available at: http://www.volkskrant.nl/vk/nl/2844/Archief/archief/article/detail/3223214/2012/03/10/De-digitale-onderwereld.dhtml (last visited on 8 August 2014).

33 See the document 'Answers of parliamentary questions with regard to the hacking of servers by the police' on 17 October 2014. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/10/18/antwoorden-kamervragen-over-het-hacken-van-servers-door-de-politie-terwijl-de-zogenaamde-hackwet-nog-niet-door-de-kamer-is-beha (last visited on 23 December 2014).

34 Translated by the author.

35 Based on art. 125i DCCP jo. 96c DCCP.

To conclude, no judgments in the Netherlands have indicated the legal basis for remote searches. However, news articles in the media and a press release from the Public Prosecution Service have made it clear that Dutch law enforcement authorities have utilised hacking as an investigative method at least four times in the past six years. The legal basis that was used for these investigations stems from the investigative power for searching a place and securing data that is stored on a computer in art. 125i DCCP. For that reason, it can be argued that an accessible legal basis is available for the investigative method of a remote search. However, as argued under A, after an analysis of the Dutch criminal procedural law, the conclusion should be that the DCCP does not provide a legal basis to conduct a *remote* search. The special investigative power in art. 125i DCCP should be read *in conjunction with the power for searching a place* and not be interpreted so extensively that it provides law enforcement authorities the power for remotely accessing a computer.[36] During a remote search, an entirely different investigative method is applied with its own specific interference with the right to privacy. The law is in my view interpreted too extensively by Dutch law enforcement authorities and the Minister of Security and Justice. Nevertheless, the legal basis for the investigative method is apparently the search and seizure of a place to secure data in computers in art. 125i DCCP. Therefore, the law should be considered as accessible.

D Public guidelines

The Public Prosecution Service's Guideline for Special Investigative Powers, the Guideline for Child Pornography Investigations, and the Guideline for the Seizure of Objects do not mention the use of a remote search. They thus provide no indication regarding the legal basis for this investigative method.

8.1.3 The use of policeware

Policeware is software that enables law enforcement officials to remotely and secretly turn a computer's functionalities on to gather evidence in a criminal investigation. For example, law enforcement officials can overcome the challenge of encryption in transit by intercepting an individual's communications 'at the source' before encryption is enabled. The use of policeware makes this possible by remotely turning a microphone on and intercepting keystrokes. The intercepted data is then returned to the law enforcement officials at a later point in time. Policeware can also be used to create a 'back door' that enables officials to remotely access a computer. Law enforcement officials can then view the computer screen through the eyes of a suspect by taking screenshots. Policeware can also be used to

36 See also J.J. Oerlemans, 'Hacking without a legal basis', LeidenLawBlog, 30 October 2014. Available at: http://leidenlawblog.nl/articles/hacking-without-a-legal-basis (last visited on 21 July 2014).

overcome the challenge of anonymity in cybercrime investigations. Once law enforcement officials gained remote access to a computer and installed the software, the software can be directed to send law enforcement officials the originating (public) IP address of the computer and other identification information.[37]

The accessibility of the legal basis for using policeware as an investigative method is examined below utilising the announced research scheme.

A Statutory law

Arguably, Dutch law enforcement authorities can install policeware on a suspect's computer using the legal basis of the special investigative power for recording private communications with a technical device.[38] Art. 126l(1) DCCP reads as follows:

"In case of suspicion of a crime as defined in art. 67(1) DCCP considering its nature and cohesion with other crimes the suspect committed seriously interfere with the legal order, a public prosecutor can, insofar the interest of investigation demands it, order a law enforcement official as meant in art. 141(b)(c), to record private communications with a technical device"[39]

This special investigative power allows law enforcement officials to record private communications using a 'technical device'. The wording of the text itself does not exclude the possibility that policeware is regarded as a technical device for recording private communications. However, as explained in the introduction to this subsection, policeware can have functionalities that go beyond just recording private communications. Therefore, if art. 126l DCCP is broadly interpreted, it can be argued that this special investigative power provides a legal basis for using policeware insofar as the policeware only records private communications (cf. Verbeek, De Roos & Van den Herik 2000, p. 155 and Koops & Buruma, p. 118 in: Koops 2007).

B Legislative history

In 1997, the Dutch legislature stated in its explanatory memorandum to the Special Investigative Powers Act that on the basis of art. 126l DCCP (recording private communications with a technical device), Dutch law enforcement officials can install a 'bug' on (1) a keyboard (to intercept keystrokes)

37 See subsection 2.4.3.

38 See art. 126l DCCP. The special investigative power for intercepting communications from public electronic communication service providers without the cooperation of the provider (see art. 126m DCCP) is not applicable, since that investigative power does not allow law enforcement officials to enter a private place in order to intercept the communications. The Dutch legislature has only made this possible for recording private communications under art. 126l DCCP (cf. Koops 2010, p. 2465).

39 Translated by the author.

and (2) a computer mouse (to intercept clicks).[40] Legislative history thus indicates that the functionalities of recording keystrokes or mouse clicks are permitted under the special investigative power for recording private communications.

Furthermore, in 2014 the Dutch Minister of Security and Justice explained in a letter to Dutch Parliament about the use of 'spyware' by Dutch law enforcement authorities that they are permitted to 'physically install' software on a computer on the legal basis of the special investigative power for recording private communications.[41] 'Physically installing the software' likely means that a (physical) search is conducted at a place, after which law enforcement officials install policeware on a computer. He further explained that the functionalities of the software are limited to recording private communications.

To conclude, legislative history indicates that the special investigative power for art. 126l DCCP to record private communications can provide a legal basis for using policeware, insofar as the software's functionalities are restricted to intercepting private communications.

C Case law

In the Netherlands, no judgments are available with regard to the practical use of policeware.[42] Several news articles have suggested that Dutch law enforcement officials utilised policeware in a child abuse investigation,[43] but the legal basis that was used to apply the investigative method has not been mentioned. It can therefore be concluded that case law does not provide an indication concerning the legal basis for this investigative method.

D Public guidelines

The Guideline for Special Investigative Powers specifies which procedures apply to the special investigative power for the interception of private communications.[44] It does not state that *software* can be used to intercept private communications, but it also does not exclude that possibility in that it consistently refers broadly to using 'a technical device'.

---

40 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 35.

41 *Kamerstukken* II 2013/14 (Proceedings of the Second Chamber), 7 October 2014, no. 202 (Answers to parliamentary questions of the Parliamentary Member Gesthuizen regarding the use of controversial spyware by the Dutch Police). Available at: https://zoek.officielebekendmakingen.nl/ah-tk-20142015-202.html (last visited on 14 May 2016). See also J.J. Oerlemans, 'Antwoord Kamervragen over het gebruik van omstreden spionagesoftware', *Computerrecht* 2014/211.

42 However, as explained in subsection 8.2.3, indications that such software is utilised in practice do exist.

43 See, e.g., NOS.nl, 'OM zette keylogger in bij Todd-zaak', 25 June 2014. Available at: http://nos.nl/artikel/666433-om-zette-keylogger-in-bij-toddzaak.html (last visited on 11 August 2014).

44 See most notably section 2.4 of the Guideline for Special Investigative Powers.

8.1.4 Section conclusion

The analyses conducted in subsections 8.1.1 to 8.1.3 can be used to assess the accessibility of the Dutch legal framework for the types of hacking as investigative methods. The results are presented below.

The investigative method of a network search is regulated as a special investigative power in the Netherlands. Network searches can be applied on the same legal basis that is used to search a place in order to gather evidence in a criminal investigation. An indication about the applicable regulations for the investigative method is thus provided. As a result, the Dutch legal framework for this investigative method is considered to be *accessible*. However, only one case that refers to the investigative method is available and the investigative method is not elaborated upon in the examined guidelines.

The investigative method of a remote search is not regulated as a special investigative power in the Netherlands. Nevertheless, a 2012 letter of the Minister of Security and Justice (following several news articles about Dutch law enforcement authorities' practical use of remote searches) indicated that the digital investigative method can be based on the investigative power to search a place in order to secure data stored on a data carrier (regulated in art. 125i DCCP). The law is considered *accessible*, since apparently the legal basis in art. 125i DCCP is used to conduct remote searches in the Netherlands.

The legal basis of the special investigative power for recording private communications is formulated in a technologically neutral manner and leaves room for the interpretation that policeware can also be used as a 'technical device' to record private communications. The explanatory memorandum to the Special Investigative Powers Act and a letter from the Dutch Minister of Security and Justice to the parliament supports the view that policeware can be applied on the legal basis of the special investigative power for recording private communications, insofar as the investigative method is restricted to that. The Dutch legal framework for this investigative method is therefore considered to be *accessible*, insofar as the method does not go beyond recording private conversations.

8.2 Foreseeability

A legal framework that is foreseeable prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which the investigative method is exercised.[45] With regard to remote searches and the use of policeware, the fact that these investigative methods are applied covertly is important. As explained in subsection 4.4.2, the ECtHR requires that the regulation of the use of covert investigative methods must be: *"sufficiently clear in its terms to give individuals an adequate indication*

45 See subsection 3.2.2 under B.

as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures".[46] Network searches cannot be applied in a covert manner. The investigative method requires law enforcement officials to conduct a search at a specific place, after which the data that is stored on interconnecting computers can be searched. At least this first part of the network search is visible to the individuals that are present at the location the initial search is conducted. Nevertheless, network search are also privacy intrusive and require detailed regulations in statutory law as a legal basis.

The analysis in section 8.1 showed that an indication is provided concerning the applicable legal basis for all three types of hacking as an investigative method. Subsections 8.2.1 to 8.2.3 now explore whether these legal bases indicate the scope of these investigative methods and the manner in which each method should be applied with sufficient clarity. Subsection 8.2.4 then draws conclusions regarding the foreseeability of this investigative method in Dutch law.

8.2.1 Network searches

The foreseeability of the legal basis for preforming network searches as an investigative method is examined below using the announced research scheme.

A Statutory law

The special investigative power for conducting a network search authorises law enforcement officials to 'investigate stored data on a computer that is located elsewhere' during a search at a specific place.[47] As explained in subsection 8.1.1, this investigative power refers back to the regulations for searches that are conducted by law enforcement officials in criminal investigations. Statutory law thus indicates the conditions that apply when conducting a network search at a particular place, which are based on where the search takes place.

However, the scope of the investigative power and the manner in which the investigative power is applied remains unclear. The special investigative power does not indicate clearly how data located on other computers can be searched when a network search is conducted. For instance, it does not specify whether law enforcement officials can use smartphone apps to search for evidence or a web browser on a suspect's computer to attempt to log in to his webmail account. The Dutch Ministry of Security and Justice stated in a report that law enforcement officials are indeed authorised to use a network search to 'log in to a server of Gmail or Dropbox to access e-mails and documents stored "in the cloud" '.[48] The special investigative power itself is for-

46 See specifically ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 26.
47 See art. 125j DCCP.
48 See the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53.

mulated so broadly, i.e., "to search for data that is located elsewhere, from the location that the search takes place, insofar this is reasonably required to uncover the truth", that the scope of the investigative method cannot be said to be indicated with precision. It is imaginable that the provision itself is formulated in such a broad manner. Yet, it requires that the scope of the investigative method is clearly restricted in other legal sources.

B Legislative history

When the special investigative power for network searches was proposed to the Dutch parliament in 1990, the Dutch legislature must have envisioned that law enforcement officials would be enabled to search computers in an internal computer network within a residence.[49] This investigative power allows these officials to access data stored on a connected external hard drive or media player during a residence search (cf. Conings & Oerlemans 2013, p. 24).

However, cloud computing and the multitudes of online services that are offered today create new dimensions for this investigative power. Network searches can now act as an alternative to data production orders, because a network search enables law enforcement officials to directly access data from a device seized from a suspect, instead of ordering the relevant online communication provider to disclose the data to them. To obtain evidence from residents of the investigating State that is located on the servers of online service providers, it may be more straightforward for law enforcement authorities to gather evidence by use of a network search than to send data production orders to online service providers that are located on foreign territory. The reason is the use of mutual legal assistance mechanisms to obtain information from online service providers on foreign territory may take several months; with a cross-border unilateral network search, the evidence can be obtained directly. This subject and the legal questions that arise are further examined in chapter 9.

The explanatory memoranda to the two Computer Crime Acts do not provide concrete examples of this special investigative power. The explanatory memorandum to the Computer Crime Act I only emphasises that the power can only be applied insofar as the persons or employees located at the place where the search is conducted are authorised to access the data stored on the interconnected computers.[50]

It can therefore be concluded that the scope of this investigative power and the manner in which the power is applied are not made clear in legislative history.

49 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90 21 551, no. 3 (explanatory memorandum Computer Crime Act I).

50 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (explanatory memorandum Computer Crime Act I), p. 27.

C Case law

No current case law discusses or evaluates the scope of the special investigative power to conduct a network search or the manner in which the special investigative power is applied. Only *one* judgment of the Appeals Court of Amsterdam has specified that using a network search may be appropriate when that search is focused solely on retrieving data that is stored on computers. This court further noted in this case that the regular regulations for the seizure of objects during a search are also appropriate for seizing computers.[51] Once law enforcement officials have seized computers, they can subsequently analyse data that is stored on them to gather evidence. No indication is provided in the judgement as to how network searches are applied in practice.

D Public guidelines

The Public Prosecution Service's Guideline for Special Investigative Powers, the Guideline for Child Pornography Investigations, and the Guideline for the Seizure of Objects, do not mention the use of a network search as an investigative method. The examined guidelines therefore do not indicate the scope of the investigative method or the manner in which the method is applied in practice.

This is remarkable. Digital evidence that consists of stored data on computers is of growing importance in criminal investigations. This is illustrated by a growing body of case law with regard to criminal investigations that features very different types of crimes.[52] As part of their evidence-gathering activities, I would expect law enforcement officials to also look for evidence on interconnected devices. Due to developments in cloud computing techniques, a substantial amount of information is stored on the servers of online service providers. Law enforcement officials should be interested in gaining access to that evidence, which they may be able to do through a computer (often that they have seized). As already pointed out under A above, only the discussion documents on search and seizure published by the Dutch Ministry of Security and Justice in 2014 mentions a broader interpretation

51 Based on art. 94 DCCP.

52 With regard to child pornography investigations, see, e.g., Rb. Maastricht 29 June 2012, ECLI:NL:RBMAA:2012:BW9971, Rb. Gelderland, 23 August 2013, ECLI:NL:RBGEL:2013:2569, Hof Leeuwarden, 1 April 2016, ECLI:NL:GHARL:2016:2600. With regard to a drug investigation, see Rb. Gelderland, 7 April 2015, ECLI:NL:RBGEL:2015:2313. With regard to a burglary and money laundering investigation, see Rb. 27 September 2013, ECLI:NL:RBDHA:2013:12297. With regard to a murder investigation, see, e.g., Hof Arnhem, 4 May 2012, ECLI:NL:GHARN:2012:BW4764 and Rb. Noord-Holland, 11 February 2014, ECLI:NL:RBNHO:2014:1026. With regard to cybercrime investigations, see, e.g., Hof Arnhem, 21 November 2006, ECLI:NL:GHARN:2006:AZ4330 (a hacking investigation), Rb. Breda, 30 January 2007, ECLI:NL:RBBRE:2007:AZ7266 (a malware investigation), Hof 's-Hertogenbosch, 12 February 2007, ECLI:NL:GHSHE:2007:BA1891 (a malware investigation), Rb. Den Haag, 2 April 2010, ECLI:NL:RBSGR:2010:BM1481 (a death threat investigation), Rb. Amsterdam, 17 February 2015, ECLI:NL:RBMNE:2015:922 (a hacking and fraud investigation), and Rb. Noord-Holland, 11 February 2016, ECLI:NL:RBNHO:2016:1023 (a bomb threat investigation).

of a network search. The authors of these documents state that law enforcement officials can use a network search to gain access to (1) e-mail stored on a web server, such as Gmail, and (2) documents stored 'in the cloud', such as in Dropbox.[53] The statutory law that regulates the investigative power itself does not exclude these two possibilities. However, this interpretation of the law is not supported by any of the other examined legal sources. In other words, ambiguity exists with regard to the foreseeability of the scope of the investigative power to conduct a network search. Research shows that the scope of the investigative power is also not clear in practice (see Koops et al. 2012b, p. 38 and Mevis, Verbaan & Salverda 2016, p. 74). However, this ambiguity regarding the scope of the investigative method is explained by these authors in connection with uncertainty with regard to the territorial restrictions of the investigative power. These questions are addressed in subsection 9.5.1 in chapter 9.

8.2.2 Remote searches

The foreseeability of the legal basis for preforming remote searches as an investigative method is examined below using the announced research scheme.

A Statutory law

Remote searches are not regulated as a special investigative power in Dutch criminal procedural law. The analysis under C in subsection 8.1.2 has shown that, the legal basis of the investigative power to 'search a place in order to secure data stored on a data carrier' in art. 125i DCCP has been used in practice to apply the investigative method. This provision refers back to investigative powers that regulate the search of a place, during which the appropriate authorities can seize objects such as computers (cf. Mevis, Verbaan & Salverda 2016, p. 27).

As an investigative method, a remote search is substantially different to the search of a place and the seizure of objects. During a remote search, hacking techniques are used to covertly access computers and evidence is subsequently secured. During a regular search and seizure, law enforcement officials physically enter a place and gather evidence. The privacy interferences that accompany the covert application of this investigative method and the gathering of data from computers simply differ from those that arise when a physical search is conducted. In my view, this investigative method merits specific legislation and its own procedural safeguards. The law is interpreted too extensively, when remote searches are based on the investigative power for searching a place (cf. Oerlemans 2011. 907-908).[54]

53 See the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53.

54 It should be noted that here the normative requirements of foreseeability and the quality of the law again become intertwined.

B Legislative history

The explanatory memoranda to both Dutch Computer Crime Acts and the Special Investigative Powers Act do not provide clarity about the scope of the investigative method of a remote search and the manner in which this method is applied.

As mentioned under B in subsection 8.1.2, the Dutch Minister of Security and Justice noted in a 2014 letter to the Dutch parliament that Dutch law enforcement authorities have obtained 'remote access to computers' in several criminal investigations.[55] It thus appears that the minister and Dutch law enforcement authorities have adopted the same interpretation of art. 125i DCCP. According to the minister, the investigative power for searching a place to conduct a computer search only grants Dutch law enforcement officials the authority to gain remote access to computers in 'special circumstances'.

However, the aforementioned statements do not clearly indicate the scope of the investigative method. As I have argued under A above, the special investigative power in art. 125i DCCP does not provide an adequate legal basis for performing remote searches. The special investigative power described in art. 125i DCCP should be read *in conjunction with the power for searching a place* and not be interpreted so extensively that it provides law enforcement authorities the power for remotely accessing a computer.[56]

C Case law

The examined cases in subsection 8.1.2 have illustrated how remote searches have been conducted to gain remote access to (1) a webmail account to access private messages detailing the shipment of drugs, (2) several servers to take over a botnet, and (3) a server to replace child pornography images with the image of a police logo. Below, a fourth case is examined that further illustrates the scope of the investigative method.[57] The case involved a death threat that was published on the Internet and illustrates how a remote search was used to determine the location of a computer and a suspect.

On 20 April 2013, the following message was posted on 4Chan.org (an online forum):

"Tomorrow, I will shoot my Dutch teacher, and as many students as I can. It will be on the news tomorrow. It's a school in a dutch city called Leiden, and for more proof, I wil be using a 9mm Colt Defender. I will be carrying a note with me when I

55 See the document 'Answers of parliamentary questions with regard to the hacking of servers by the police' on 17 October 2014. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/10/18/antwoorden-kamervragen-over-het-hacken-van-servers-door-de-politie-terwijl-de-zogenaamde-hackwet-nog-niet-door-de-kamer-is-beha (last visited on 23 December 2014).

56 See also J.J. Oerlemans, 'Hacking without a legal basis', *LeidenLawBlog.nl*, 30 October 2014. Available at: http://leidenlawblog.nl/articles/hacking-without-a-legal-basis (last visited on 21 July 2014).

57 See Rb. Den Haag, 19 November 2013, ECLI:NL:RBDHA:2013:15617.

go into the school which will explain why I did it. If the message of the note will not be published, a friend of mine with the post here on 4chan a day later. Oh, and I'm using a proxy, the police is not gonna find me before tomorrow."[58]

Dutch law enforcement authorities took this death threat seriously and launched an investigation. Here it is important to note that 4Chan is a so-called 'image board' where individuals can post messages without disclosing their real names or nicknames; the above message was also signed 'anonymous'. However, these online services do log the IP addresses of users who post to the image board. Law enforcement authorities can obtain this information by issuing a data production order.[59] In this case, the IP address was assigned to a router at a youth hostel in Costa Rica (not a proxy server, as the author claimed in the message).[60] However, officials felt it was necessary to obtain remote access to the router to validate that the IP address belonged to the hostel. They reportedly accessed the router using 'admin' as both the login name and password.[61] The suspect turned himself in and flew back to the Netherlands, after which he was arrested and successfully prosecuted by Dutch law enforcement authorities.[62] In the judgement, the Dutch judges did not address the lacking legal basis for the remote search that was conducted.[63] The trial lawyers did not object to this investigative activity.

When all of the above information and the examined cases in subsection 8.1.2 are taken into account, it can be concluded that case law shows that a remote search has been conducted to remotely access (1) an online account, (2) a router of a youth hostel, (3) a botnet's command-and-control server, and (4) hidden services on Tor. It is thus clear that this investigative method is currently being applied to access many different types of computers for a variety of purposes in the absence of detailed regulations to restrict its scope. This research result suggests that the Dutch legal framework is currently not foreseeable in the context of this investigative method.

58 The original message was mentioned in the judgment (including spelling and grammar errors). See Rb. Den Haag, 19 November 2013, ECLI:NL:RBDHA:2013:15617.

59 See chapter 6. In this case, mutual legal assistance may have been required to obtain data from a foreign hosting provider.

60 See Joost Schellevis, 'OM: politie brak in op router vanwege "acute dreiging" ', *Tweakers*, 6 November 2014. Available at: http://tweakers.net/nieuws/92427/om-politie-brak-in-op-router-vanwege-acute-dreiging.html (last visited on 14 April 2014). It should be noted that jurisdictional issues may be involved with this investigative activity. These issues are further addressed in chapter 9.

61 See Joost Schellevis, 'OM: politie brak in op router vanwege "acute dreiging" ', *Tweakers*, 6 November 2014. Available at: http://tweakers.net/nieuws/92427/om-politie-brak-in-op-router-vanwege-acute-dreiging.html (last visited on 14 April 2014).

62 See RTLNieuws.nl, 'Verdachte Leiden gevonden in Costa Rica', 26 April 2013. Available at: http://www.rtlnieuws.nl/nieuws/binnenland/verdachte-leiden-gevonden-costa-rica (last visited on 26 April 2016).

63 See Rb. Den Haag, 19 November 2013, ECLI:NL:RBDHA:2013:15617.

D Public guidelines

As explained in subsection 8.1.2, the Public Prosecution Service's Guideline for Special Investigative Powers, the Guideline for Child Pornography Investigations, and the Guideline for the Seizure of Objects do not mention remote searches as an investigative method. Therefore, no indication regarding the scope of the investigative method or the manner in which the method is applied is available in the examined guidelines.

8.2.3 The use of policeware

The foreseeability of the legal basis for using policeware as an investigative method is examined below utilising the announced research scheme.

A Statutory law

In Dutch criminal procedural law, the special investigative power for intercepting private communications allows law enforcement officials to record private communications using a 'technical device'.[64] This power specifies in detail under which conditions it can be applied. Additional requirements are applicable when a technical device is installed inside a residence. A Dutch public prosecutor can order the application of the special investigative power for intercepting private communications using a technical device outside of a residence after obtaining a warrant from an investigative judge. The power can be applied for a maximum period of four weeks, which can be extended for another four weeks.[65] In addition, the individual involved must be suspected of a crime as defined in art. 67(1) DCCP that seriously infringes upon the legal order. The application of this investigative method must also be essential to furthering the criminal investigation.[66] When a technical device is to be installed within a residence, the relevant crime must also be sanctioned by a prison sentence of at least eight years.[67]

With regard to the scope of the investigative method, it is important to note that statutory law does not clarify what a technical device entails. Statutory law also does not indicate in which manner the investigative method can be applied. However, it is clear that a physical technical device can be installed by breaking into a place. Policeware can be installed in a similar manner by 'breaking into' (i.e., hacking) a computer.

To conclude, this special investigative power indicates under which conditions it can be applied, but not the investigative power's scope or the manner in which the investigative method can be applied in a digital context.

64 See art. 126l DCCP. See also subsection 8.1.3 under A.
65 See art. 126l DCCP.
66 See art. 126l(1) DCCP.
67 See art. 126l(2) DCCP.

B Legislative history

In 1997, the Dutch legislature stated in its explanatory memorandum to the Special Investigative Powers Act that Dutch law enforcement officials can install technical devices on keyboards (to intercept keystrokes) and computer mice (to intercept mouse clicks).[68] This special investigative power can only be applied insofar as private communications are recorded for evidence-gathering purposes. The explanatory memorandum explains that the term 'private communications' is interpreted broadly, namely to include data that is sent between two parties.[69] When a computer is connected to the Internet, law enforcement officials can thus intercept network traffic that takes place between computers that is then regarded as private communications. The technical device that is utilised to apply this special investigative power must meet specifications included in lower regulations. These specifications require Dutch law enforcement officials to, for instance, send the intercepted communications through a secure connection and store the data in a secure place to avoid data manipulation.[70]

Interestingly, the explanatory memorandum explicitly mentions how a technical device can enable law enforcement officials to intercept communications between two parties *before* the information is encrypted.[71] This description resembles an important functionality of policeware, which can be used to intercept data (in the form of keystrokes or voice messages), before it is encrypted by online service providers.[72] However, the explanatory memorandum does not explicitly mention that *software* can be utilised to intercept private communications.

Taking the above into account, it can be concluded that legislative history provides information regarding the scope of the investigative method and the manner in which the investigative method can be applied. Although this legislative history is over 20 years old, the text is formulated in a technologically neutral manner and may cover certain functionalities of using policeware as an investigative method. However, certain questions remain unaddressed, such as whether the software's capacity to take screen shots with policeware can be used as part of the special investigative power for recording private communications.

C Case law

As explained in subsection 8.1.3, no judgments concerning the legitimacy of the use of policeware are available. However, news articles in the media about a pending case reveal that Dutch law enforcement officials report-

68 See also subsection 8.1.3.

69 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 37.

70 See art. 13 and 14 of the Besluit technische hulpmiddelen, *Stb.* 2013, 49.

71 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 36.

72 See subsection 2.4.3.

edly used policeware in an online child abuse case.[73] The use of policeware enabled them to (1) log chat conversations by intercepting keystrokes and (2) take screenshots of the suspect's computer screen.[74] After analysing leaked documents, journalists concluded that Dutch law enforcement authorities purchased 'FinFisher' policeware from the German company Gamma International.[75] FinFisher software indeed has the capacity to log keystrokes and take screen shots. In addition, the software reportedly has an option that allows law enforcement officials to turn a computer's microphone on and monitor Skype conversations before information is encrypted, thereby overcoming the obstacle of encryption in transit in criminal investigations.[76] The software reportedly even allows officials to extract files from a hard disk and gain remote access to a computer system for 'live remote forensics'.[77]

As of the time of writing (October 2016), it is unclear whether the policeware was remotely installed on the suspect's computer and which of the software's functionalities were utilised, although news articles suggest that screen shots were taken. This functionality appears to be broader than the Dutch legislator anticipated within the special investigative power for recording private communications under art. 126l DCCP.

D Public guidelines

The Guideline for Special Investigative Powers devotes an entire section (section 2.5) to the application of and procedures which to apply the special investigative power for the recording private communications.[78] The guideline largely repeats the relevant parts of legislative history. It also specifies that when a technical device is installed in a residence, a public prosecutor must consult the Public Prosecution Service's special advisory commis-

73 The case concerned a suspect who enticed under-aged girls to perform sexual activities over the Internet. One of these girls committed suicide, which led to unrest in her home country of Canada. See, e.g., Patrick White and Jane Taber, 'Dutch police arrest suspect in the Amanda Todd case', *The Globe and Mail*, 17 April 2014. Available at: http://www.theglobeandmail.com/news/british-columbia/amanda-todd/article18055474/ (last visited on 11 August 2014).

74 See, e.g., NOS.nl, 'OM zette keylogger in bij Todd-zaak', 25 June 2014. Available at: http://nos.nl/artikel/666433-om-zette-keylogger-in-bij-toddzaak.html (last visited on 11 August 2014).

75 See Michael Persson, 'Politie gebruikt mogelijk omstreden spionagesoftware', *Volkskrant*, 8 August 2014. Available at: http://www.volkskrant.nl/vk/nl/2694/Tech-Media/article/detail/3715207/2014/08/08/Politie-gebruikt-mogelijk-omstreden-spionagesoftware.dhtml (last visited on 11 August 2014).

76 See subsection 2.4.1 with regard to the challenge of encryption in transit in criminal investigations. Skype encrypts network traffic by default. Law enforcement officials are presumably unable to read the contents of Skype conversations when the information is intercepted using a wiretap at a public telecommunication service provider (cf. Oerlemans 2012, p. 27).

77 See Morgan Marquis-Boire, 'From Bahrain With Love: FinFisher's Spy Kit Exposed?', *Citizen Lab*, 25 July 2012. Available at: https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/ (last visited on 10 July 2014).

78 See section 2.5 of the guideline for special investigative powers of 2014.

sion.[79] This commission will then advise on the desirability of using this special investigative power in a particular case. The Guideline for Special Investigative Powers does not mention whether policeware is understood as a technical device and provides no specifications with regard to the functionalities of technical devices. The guideline therefore only provides additional information about the manner in which the investigative method is applied by explaining that it is necessary to consult the special advisory commission.

8.2.4 Section conclusion

The analyses conducted in subsections 8.2.1 to 8.2.3 can be used to assess the foreseeability of the Dutch legal framework in criminal procedural law with regard to the examined types of hacking as an investigative method. The results are summarised below.

Despite the detailed provisions that exist in Dutch criminal procedural law concerning the application of network searches as an investigative method, the legal basis of this investigative method is considered *not foreseeable*. The reason is that none of the examined sources in law indicate the scope of network search or the manner in which the investigative method is applied in practice. A discussion document from the Dutch Ministry of Security and Justice boldly stated that network searches also enables law enforcement officials to access online accounts. However, the examined legal sources do not indicate that this application is possible. Most of the information available is from legislative history that is over 25 years old. This leaves ambiguity with regard to the scope of network searches and the manner in which the investigative method is applied in practice.

The legal basis for performing a remote search is considered *not foreseeable*. Dutch law does not explicitly indicate the legal basis for this investigative method. According to the Dutch Minister of Security and Justice at the time, this method can be based on the investigative power to search a place in order to secure data stored on a data carrier. However, this investigative power refers back to an existing power for searching places and seizing objects that are located in that place. Remote searches go a significant step further, given that computers are accessed covertly. The power for searching places and seizing objects is meant for the physical world. I argued that the referenced provisions in Dutch criminal procedural law do not authorise law enforcement officials to hack into computers and secure evidence remotely. Furthermore, the privacy interferences that accompany

79 In a particularly pressing situation, a public prosecutor can choose to apply the special investigative power without advice form the special commission after obtaining a warrant from an investigative judge. A special team of the Dutch police that is tasked with installing the device will then examine whether its installation is feasible from technical and tactical perspectives.

remote searches are also different from those that accompany regular computer searches. As such, remote searches as an investigative method should be regulated in distinct specific provisions in the DCCP.

Based on statutory law and the explanatory memorandum to the Special Investigative Powers Act, it can be argued that policeware can based on the special investigative power to record private communications. The examined legal sources however do not clarify which functionalities of policeware can be applied. For example, it remains unclear whether the special investigative power authorises law enforcement officials to take over a suspect's computer and subsequently take screen shots or gain remote access to a computer system and conduct a remote search. The legal basis for this investigative method in Dutch law is therefore considered *not foreseeable* for this investigative method.

8.3 Quality of the law

The normative requirement regarding the quality of the law, means that the ECtHR can specify the level of detail required for the description the investigative power and the minimum procedural safeguards that must be implemented vis-à-vis a particular method that interferes with the right to privacy. The detail that the ECtHR requires in the law and procedural safeguards depends on the gravity of the privacy interference that takes place.[80]

The desired quality of the law for hacking as an investigative method, was determined in subsection 4.4.4. An overview of the desired quality of the law for all three types of hacking as an investigative method is provided in Figure 8.2.

80 See subsection 3.2.2 under C.

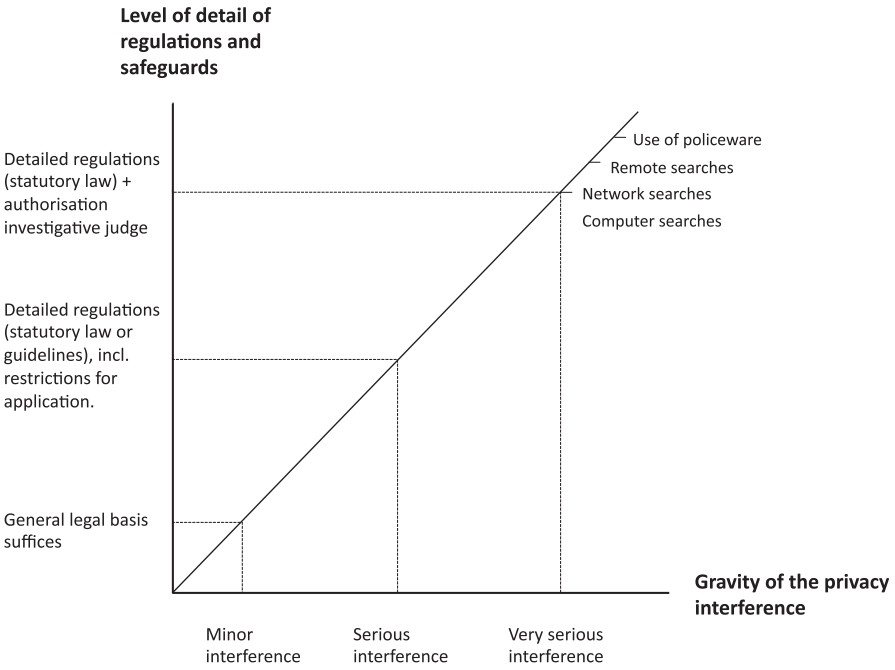

Figure 8.2: The quality of the law for hacking as an investigative method.

Figure 8.2 illustrates how all types of hacking as an investigative method are considered as highly privacy intrusive investigative methods that require detailed regulations in statutory law with at the procedural safeguards of authorisation of an investigative judge. More specifically, the analysis showed that network searches are very intrusive investigative methods, because computers within a network can contain large amounts of personal information of individuals. Remote searches and the use of policeware are more privacy intrusive than network searches, given that they are applied covertly. As covert applications of investigative methods are accompanied by higher risks of abuse by law enforcement authorities, they merit stronger procedural safeguards (more specifically, a warrant from an investigative judge). The use of policeware is the most intrusive investigative method that is examined in this study, because it combines several intrusive investigative methods in one. The investigative method can be considered as a combination of a computer search, sneak-and-peek operation, and wiretapping. The high intrusiveness of the investigative method and broad scope of the investigative method merit that the investigative method is regulated in detail with the procedural safeguard of a warrant, with clear restrictions concerning the duration and functionalities of the policeware.

In subsections 8.3.1 to 8.3.3, the quality of the law of the Dutch legal framework with regard to the three types of hacking as an investigative method is compared to the desired quality of the law. Subsection 8.3.4 then draws conclusions as to whether the Dutch legal framework for hacking as an investigative method meets the desired quality of the law.

8.3.1 Network searches

The desirable quality of the law for network searches has been identified as detailed regulations in statutory law, with the procedural safeguard of a warrant that is issued by an investigative judge.[81]

As defined in Dutch criminal procedural law, the special investigative power for a network search refers back to existing investigative powers to conduct a search at a particular place. The same conditions thus apply to both network searches and searches of particular places and the subsequent seizure (and analysis) of computers. Different regulations and conditions from Dutch criminal procedural law apply depending on where a search is conducted.[82]

This differentiated legal regime for searching computers based on their location is not appropriate (cf. Koops et al. 2012b, p. 59 and Conings & Oerlemans 2013, p. 26). Computers are not regular objects that can be seized during a search of a place. They often store large amounts of personal information that can be analysed with software. Seizing a computer and subsequently searching the data stored they contain therefore heavily interferes in an individual's private life (cf. Groothuis & de Jong 2010, p. 280 and Conings & Oerlemans 2013, p. 26). Individuals should be protected from arbitrary governmental interference during computer and network searches, no matter where the computer is located. The Dutch legal framework for network searches therefore does not currently meet the desired quality of the law. The special investigative power for network searches (which should not refer back to investigative powers for conducting searches at particular places) also requires the procedural safeguard of an investigative judge to help determine which computers should be accessed and balance the purpose for

81 See subsection 4.4.4.

82 See subsection 8.1.1. See also Figure 8.1 in the introduction. In two cases, Dutch judges found that the current Dutch regulations to search a place, seize computers, and subsequently search the data stored on computers were in violation with art. 8 ECHR. See Hof Arnhem-Leeuwarden, 22 April 2015, ECLI:NL:GHARL:2015:2954, m.nt. J.J. Oerlemans, *Computerrecht* 2015/127 and Rb. Noord-Holland, 4 June 2015, ECLI:NL:RBNHO:2015:4660. However, a majority of Dutch courts have since stated that the Dutch regulations for computer searches, more specifically art. 94 DCCP, clearly provides a legal basis for seizing computers (during a search) and subsequently analysing the data stored on them. See, e.g., Rb. Amsterdam, 18 June 2015, ECLI:NL:RBAMS:2015:4024, Hof Amsterdam, 13 November 2015, ECLI:NL:GHAMS:2015:5007, Rb. Overijssel, 1 March 2016, ECLI:NL:RBOVE:2016:708. Interestingly, the Court of Amsterdam stated that the possibility for suspects to object to a computer search suffices to meet the preferred involvement of an investigative judge by the ECtHR (see Hof Amsterdam, 24 February 2016, ECLI:NL:GHAMS:2016:579). In my view, the ECtHR prefers a warrant from an investigative judge as a procedural safeguard for computer searches. It is possible the Dutch Supreme Court will decide on the issue, insofar as the Dutch legislature does not amend the law sooner. See further J.J. Oerlemans, 'Rechtspraak verdeeld over rechtmatigheid van het doorzoeken van smartphones', *Computerrecht* 2016, no. 3, p. 204-205.

gathering evidence with the interference to the involved individual's rights and freedoms, regardless of where computers have been seized.

It is worth noting that when the special investigative power for network searches was proposed to the Dutch parliament in 1990, the power was described as '*the most far reaching investigative power with regard to computer investigations*' in criminal procedural law.[83] Despite the emphasis on this investigative power's intrusiveness in terms of privacy, *no* examples of the concrete application of this method are provided in legislative history and almost no relevant case law is available. Considering both how technology has advanced and the recent case law of the ECtHR on computer searches, it appears appropriate to rethink the Dutch legal regime for computer and network searches.

8.3.2 Remote searches

The desirable quality of the law for remote searches has been identified as detailed regulations in statutory law, with the procedural safeguard of a warrant issued by an investigative judge.[84]

A specific legal basis in the DCCP is required for remote searches, given that the investigative method interferes with an individual's right to privacy in a very serious manner. The covert use of investigative methods poses greater risks of a governmental abuse of power. Bearing both the serious privacy interference and the criminal procedural legality principle in mind, it follows that the Dutch legislature should regulate this investigative method as a special investigative power in Dutch criminal procedural law (cf. Oerlemans 2011, p. 899-901).[85] Currently (as of October 2016), no such special investigative power is available in the DCCP. The Dutch legal framework regulating remote searches therefore does not currently meet the desired quality of the law.

8.3.3 The use of policeware

The desirable quality of the law for using policeware consists of (1) detailed regulations for the investigative method, (2) a warrant requirement, and (3) restriction of the duration and functionalities as procedural safeguards (cf. Oerlemans 2011, p. 908).[86]

Within the Dutch legal framework, stringent conditions already apply for applying the special investigative power for recording private communications with a technical device. The Dutch legislature reasoned at the time (1996) that applying this special investigative power seriously interferes

83 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90 21 551, no. 3 (explanatory memorandum Computer Crime Act I), p. 27.
84 See subsection 4.4.4.
85 See subsection 4.4.4.
86 See subsection 4.4.4.

with the right to privacy.[87] Although the Dutch legislator may have had the application of a different investigative method in mind, the strict requirements to apply the special investigative power appear also suitable for the use of policeware. In other words, the procedural safeguards that apply to the use of the special investigative power for recording private communications meet the desired quality of the law in relation to the use of policeware. A warrant must be obtained and the application of the investigative method is restricted in duration. The heightened proportionality principle that applies to this power should be translated in practical terms to restrictions concerning which functionalities of policeware may be used by law enforcement authorities.

However, note that the special investigative power for recording private communications does not indicate the scope of the use of policeware and the manner in which this software can be used in sufficient detail. Here, the normative requirements of foreseeability and the quality of the law are clearly intertwined. When all of the normative requirements are taken into consideration, the current regulations are therefore still not in 'accordance with the law', as meant in art. 8 ECHR.

8.3.4 Section conclusion

This section compared the quality of the law of the Dutch legal framework for criminal procedural law with the desirable quality of the law as determined in subsection 4.4.3. The desired quality of the law for the investigative method was visualised in Figure 8.2 in the introduction of this section. The results concerning whether the Dutch legal framework for hacking as investigative method meets the desired quality of the law are summarised below.

The Dutch legal framework for network searches *does not meet the desirable quality of the law*. The detailed regulations and corresponding procedural safeguards that apply for network searches are differentiated based on the location that network searches are conducted, which is undesirable. Computers are not regular objects, as they can contain large amounts of diverse information that should be sufficiently protected. A single investigative power should therefore apply for network searches with a warrant requirement as a procedural safeguard, regardless of where a computer was seized.

No specific legal basis for remote searches exists in Dutch criminal procedural law. Instead, the investigative power for searching a place and conducting computer searches in art. 125i DCCP refers back to existing powers for searching a place and seizing computers. These procedural safeguards in these regular search and seizure power differentiate based upon the location of the place the search is conducted. The investigative method should be regulated by a single investigative power with the procedural safeguard of a warrant from an investigative judge. Since this quality of the law is not

87 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 38.

met, the Dutch legal framework for the investigative method *does not meet the desirable quality of the law*.

The Dutch legal framework for the use of policeware cannot be considered 'in accordance with the law' as meant in art. 8 ECHR, due to ambiguity with regard to the scope of the use of policeware and the manner in which this software is utilised. However, *the quality of the law is adequate*, since a single special investigative power currently applies to using the investigative method using the maximum safeguards available in Dutch criminal procedural law. The procedural safeguards include a restriction of the duration of the use of policeware and a heightened proportionality principle that translates to a restriction of the functionalities of policeware that can be used.

8.4 Improving the legal framework

This section discusses the extent to which the DCCP can be improved in order to provide an adequate legal framework for regulating hacking as an investigative method. A legal framework is considered adequate when (1) it is accessible, (2) it is foreseeable, and (3) the desired quality of the law is met. The results of the analyses of the three normative requirements in sections 8.1 to 8.3 are summarised in Table 8.1.

Normative requirement	Network searches	Remote searches	The use of policeware
Accessible	✓	✓	✓
Foreseeable	✗	✗	✗
Meets the desirable quality of the law	✗	✗	✓

Table 8.1: Representation of the research results in sections 8.1 to 8.3 (✓ = adequate, ✗ = not adequate).

Table 8.1 shows that foreseeability is lacking in relation to the application of the three types of hacking examined in this chapter. The current regulations on which the various types of hacking are based were developed over two decades ago, and are now being applied in a different era. In 1997, the Dutch legislature stated in its explanatory memorandum to the Special Investigative Powers Act that *"new investigative methods will be developed that interfere with the right to privacy in new manners"*.[88] The use of a hacking is one such new investigative method that interferes with the right to privacy in a serious and novel manner.

88 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 11.

Furthermore, recent ECtHR case law with regard to computer searches indicates that detailed regulations are desirable for computer searches and that a warrant from an investigative judge is preferably applicable. Given that hacking as investigative method is even more privacy infringing than computer searches, it is necessary to amend the Dutch legal framework to adequately regulate its application.

Subsections 8.4.1 to 8.4.3 further examine the three types of hacking used as investigative methods and identify how each should be regulated.

8.4.1 Network searches

Network searches are regulated as a special investigative power within a specific provision of Dutch criminal procedural law. The Dutch legal framework can thus be considered as accessible. However, the scope of the investigative methods and the manner in which they are executed are unclear, due to an outdated description of the investigative method in legislative history, lack of case law, and no direction from guidelines. Currently, the procedural safeguards depend on the location the investigative method is applied, which is not desirable. It would be appropriate to incorporate a requirement for a warrant from an investigative judge in connection with the special investigative power for conducting network searches. Therefore, the special investigative power for a network search should be amended and incorporate warrant from an investigative judge as a procedural safeguard, regardless of where a computer was seized (*Recommendation 1).*

In 2015, the Dutch Minister of Security and Justice made clear that he does not regard the current legal regime for computer searches as adequate.[89] Considering the large amounts of information that are stored on computers and the software that is available to quickly analyse all of the available data, the Dutch minister suggested that a legal threshold that involves a 'higher authority' than a law enforcement official is appropriate.[90] Such an amendment may also lead to higher procedural safeguards for network searches, given that the regulations for computer and network searches are so closely intertwined.

However, due to objections from the Dutch police and Public Prosecution Service concerning the reform of the legal regime for computer searches, further research was deemed desirable to examine the 'consequences

89 Letter of 30 September 2015 regarding the modernisation of the DCCP, p. 83. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (last visited on 3 October 2015).

90 Letter of 30 September 2015 regarding the modernisation of the DCCP, p. 83. The threshold of a law enforcement official only applies when a computer is seized after a vehicle is searched (see art. 94b DCCP).

for law enforcement practice'.[91] The report that followed from Mevis, Verbaan, & Salverda (2016) noted that in current Dutch law enforcement practice, computers are seized as regular objects during the search of a place. Most often, a public prosecutor or investigative judge authorises the search and seizure of computers (see Mevis, Verbaan, & Salverda 2016, p. 52). The report's authors conclude that no uniform policy exists with regard to the seizure and analysis of data that is stored on computers in the Netherlands (Mevis, Verbaan, & Salverda 2016, p. 78). As a result, the investigative method is applied in diverse manners. The authors of the report recommend that the Dutch legislature should create extra safeguards for computer searches when they deem it necessary (see Mevis, Verbaan, & Salverda 2016, p. 79).

The report does not extensively describe developments in digital forensic technology that enable law enforcement authorities to thoroughly analyse all of a computer's stored contents, as this was beyond its mandate. The report also did not take into consideration future developments or provide new information regarding the application of network searches and the possibilities of gathering information from cloud services. A basic understanding of these factors and their impact on both evidence-gathering activities and the involved individuals' rights and freedoms is required to adequately assess how Dutch law can regulate computer and network searches.

Nevertheless, it appears that the legislature will propose new regulations for computer searches based on the report's results.[92] The contents of these regulations are still unclear. The Dutch Minister of Security and Justice has not stated that the heightened procedural safeguard of a warrant from an investigative judge will be introduced for computer searches or that authorisation of a public prosecutor will suffice.

Considering recent developments in ECtHR case law with regard to computer searches – to which the Dutch legislature does not refer in official documentation regarding its plans – the procedural safeguard of a warrant requirement appears appropriate from a human rights perspective. Of course, a higher administrative burden for law enforcement officials is expected if a warrant from an investigative judge is required to seize and analyse a computer. However, an investigative judge can check whether public prosecutors have taken sufficient measures to narrow a search down to relevant information. It is imaginable that the evidence must be first secured and filtered using software before the actual search is conducted.

91 Letter of 30 September 2015 regarding the modernisation of the DCCP, p. 84. See also page 8 of the advice of the Dutch police with regard to the proposal to modernise the DCCP. Available at: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/09/30/tk-modernisering-wetboek-van-strafvordering-advies-politie/tk-modernisering-wetboek-van-strafvordering-advies-politie.pdf (last visited on 30 September 2015).

92 See the letter of 29 June 2016 to the Dutch parliament (*Kamerstukken II* 2015/16, 29279, no. 331) concerning the legislation program of Modernising Criminal Procedural Law.

An investigative judge may have more distance with regard to the criminal case and may thus be able to help balance the interests involved. The Dutch Prosecution Service should also consider developing more detailed procedures for computer and network searches to include in its guidelines.[93]

8.4.2 Remote searches

Efforts to regulate remote searches in the DCCP began as early as 2009. The Dutch Minister of Security and Justice stated that investigating cybercrime had become 'extraordinarily difficult' due to encryption techniques and anonymising software.[94] In November 2010, the minister promised to regulate hacking as an investigative method within the Dutch national legal framework and to introduce a new bill.[95] However, no bill was introduced in the following years. In 2013, a concept bill for a new Computer Crime Act (i.e., the Computer Crime Act III) was published, with an accompanying explanatory memorandum that detailed the plans of the Dutch legislature to introduce hacking as a special investigative power in Dutch criminal procedural.[96] The proposal for the Computer Crime Act III was published on 22 December 2015.[97] The regulations for network searches in the DCCP remain untouched in the bill.

The Computer Crime Act III aims to regulate hacking as an investigative method by introducing a new special investigative power in art. 126nba DCCP. This article is supposed to provide a new legal basis for remotely accessing 'automated devices' (computers). Under the proposed investigative power, law enforcement officials can gain remote access to a computer and then conduct the following investigative activities:

(1) ascertain or identify the characteristics of a computer or computer user;
(2) intercept private communications and generated network traffic;
(3) observe the movements of a computer and its user by monitoring GPS data;

93 Inspiration can be drawn from the guideline of the Dutch Consumer and Market Authority ('Autoriteit Consument en Markt'). See 'ACM Werkwijze digitaal onderzoek 2014', 11 February 2014. Available at: https://www.acm.nl/nl/publicaties/publicatie/12594/ACM-Werkwijze-digitaal-onderzoek-2014/ (last visited on 7 May 2016).

94 *Kamerstukken II* 2008/09 (Proceedings of the Second Chamber), 28 684, no. 232, p. 2-3.

95 *Kamerstukken II* 2010/11, 25 November 2010, Answers to parliamentary questions of Recourt, no. 2010Z15331.

96 See the article on the official website of the Dutch government 'Opstelten versterkt aanpak computercriminaliteit', 1 May 2013. Available at: http://www.rijksoverheid.nl/nieuws/2013/05/02/opstelten-versterkt-aanpak-computercriminaliteit.html (last visited on 4 January 2014).

97 See 'Wetsvoorstel Computercriminaliteit III'. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/wetsvoorstel-computercriminaliteit-iii (last visited on 30 December 2015).

(4) conduct a remote search and copy data; and
(5) make data remotely inaccessible.[98]

If the bill is eventually adopted as legislation, an *accessible* legal basis for applying a remote search as an investigative method will be available in Dutch criminal procedural law.

However, the current proposal can be criticised with regard to its *foreseeability*, more particularly the *scope* of the proposed special investigative power. For example, one can argue that the term 'automated devices' – to which law enforcement officials can gain access – is rather broad. Automated devices encompass a wide range of items, such as (a) personal computers, (b) smartphones (which are also essentially computers), (c) wearable computing devices, (d) smart refrigerators, and (d) interconnected cars.[99]

At the same time, the rapid pace of technological developments means that new legislation must also be technologically neutral. Specifically with regard to the term 'computer', it will be complicated – if not impossible – to narrow the scope of the definition. For example, restricting the special investigative power to *personal* computers creates uncertainty concerning the question which computers are regarded as 'personal'. For instance, individuals will regard e-mails stored on the servers of a webmail provider as personal, but are those servers – which are owned by a private company – considered 'personal computers'? As a result, the technologically neutral term of 'automated device' is ultimately preferable.

Nevertheless, if the rapid advancements of new technologies and the list of investigative activities provided above are taken into account, it is imaginable that law enforcement officials may find it necessary to hack all kinds of computers (1) for identification purposes, (2) to intercept communications, (3) to track the movements of individuals, (4) to secure data as evidence, or (5) to make data (and thereby possibly computers themselves) inaccessible. It is thus difficult to oversee the scope of this investigative method in the (near) future. Of course, the rationale for creating the proposed special investigative power is essentially to (1) overcome the challenge of anonymity in cybercrime investigation, (2) overcome the challenges of encryption, and (3) collect data that is located 'in the cloud' (i.e., on servers from online service providers that are often housed on foreign territory).[100] The issue is that the proposed special investigative power for hacking as an investigative method is not restricted to overcome these challenges, but leave room for other applications. The proposed special investigative power is not

98 See the proposed art. 126nba DCCP, *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 2, p. 5-6 and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 21-31.

99 See section 2.1 with regard to the definition of computers.

100 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 6-15.

restricted to the distinction made for hacking as an investigative method, which subdivides the method into (1) network searches, (2) remote searches, and (3) the use of policeware.

Taking the above observations with regard to the foreseeability of the proposed investigative power into account, my view is that it is desirable to narrow the scope of the investigative method (*Recommendation 2).* The special investigative power can be limited to those applications of hacking that the Dutch legislature truly deems 'necessary in a democratic society'. These applications should then be explained more concretely in legislative history and lower regulations. Furthermore, guidelines from the Public Prosecution Service can indicate the scope of the special investigative power and the manner in which it is applied in a concrete manner.[101]

The proposed new special investigative power in art. 126nba DCCP *meets the desirable quality of the law* for regulating remote searches. This special investigative power is restricted by only allowing its application for crimes stipulated in art. 67 DCCP that 'seriously infringe the legal order' and 'only insofar essential to furthering the criminal investigation'.[102] A public prosecutor must authorise the application of the investigative method. In addition, a special commission of the Public Prosecution Service must be consulted by a public prosecutor before the proposed special investigative power can be applied. Furthermore, a warrant from an investigative judge is required and the warrant's authorisation for applying the special investigative power for remotely accessing computers is restricted to a maximum period of four weeks, which can be extended for another four weeks.[103]

8.4.3 The use of policeware

The use of policeware can arguably already be based on the legal basis of the special investigative power for recording private communications under Dutch law. As such, the regulations for this investigative method are considered accessible. However, the applications of policeware are potentially broader than the special investigative power for recording private communications, since they can also enable law enforcement officials to take a sus-

101 The answer to this question is also political in nature. Based on chapter 2, it can be argued that (1) network searches, (2) remote searches, and (3) the use of policeware, are necessary instruments for law enforcement authorities to overcome the challenges of anonymity and encryption in cybercrime investigations. Whether other applications of hacking can be considered as 'necessary' requires further analysis (including of their backgrounds).

102 Specifically, the applications of remotely turning a GPS signal on and making data remotely inaccessible are restricted to criminal investigations with regard to crimes with a minimum prison sentence of at least eight years and crimes stipulated by lower regulations, such as hacking, malware, distributing child pornography, and grooming. See art. 126nba(1)(c) DCCP and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 29.

103 See the proposed art. 126nba DCCP and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 31-34.

pect's computer over and subsequently take screen shots or gain remote access to the computer system to enable a remote search. It is therefore appropriate to place the use of policeware under the proposed special investigative power for hacking described above as an investigative method.

The use of policeware (as regulated in the proposed special investigative power) can significantly contribute to law enforcement officials' arsenal for overcoming the challenges related to anonymity and encryption. The use of policeware can enable law enforcement officials to overcome the challenge of anonymity, because the software can be directed to send the originating IP address and other identification information about the suspects' computer to law enforcement officials.[104] This investigative power can also enable officials to monitor a suspect's computer behaviours at the source, before network traffic is encrypted (cf. Abate 2011, p. 124).[105] In addition, the keylogging functionality can enable officials to acquire the password a suspect uses to encrypt data and access online services (cf. Fox 2007, p. 828),[106] which they can subsequently use to decrypt data and access information that may not be obtained using other investigative methods. The proposal creates an *accessible* legal basis for the use of policeware with the (additional) functionalities to overcome the challenges of anonymity and encryption in cybercrime investigations.

However, the *foreseeability* of the proposed special investigative power can be improved. Throughout the explanatory memorandum to the Computer Crime Act III, it is implied that policeware will have the following functionalities: (1) recording sounds (by remotely turning a computer's microphone on), (2) logging keystrokes, (3) taking screenshots, (4) remotely gaining access to computers and searching files and folders, and (5) turning a device's GPS signal on.[107] However, the explanatory memorandum also leaves room for other functionalities. Instead, a limited list of functionalities of policeware should be provided by the legislator (*Recommendation 3*). The explanatory memorandum should further elaborate these functionalities (in terms of both their scope and the manner in which they are applied). Furthermore, the functionalities of policeware should be mentioned in both Public Prosecution Service guidelines and lower regulations concerning the use of technical devices. This would ensure that the scope of the special investigative power and the manner in which the power is applied are adequately regulated.

104 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 19-20.

105 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 10.

106 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 21.

107 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 23, 25-26, 28-30, and 34.

The proposed special investigative power in art. 126nba DCCP *meets the desirable quality of the law* for the use of policeware. As explained in subsection 8.4.2, stringent requirements apply for utilising the proposed investigative power. In relation to the warrant from an investigative judge and the proportionality test, it is important that Dutch law enforcement authorities explain which functionalities of policeware they are going to use. The explanatory memorandum to the Computer Crime Act III indeed confirms that a public prosecutor's request for a warrant to use policeware must state which functionalities of the deployed policeware will be used.[108]

8.5 Chapter conclusion

The aim of this chapter was to determine how the legal framework in Dutch criminal procedural law can be improved to adequately regulate hacking as an investigative method (RQ 4d). To answer the research question, the Dutch legal framework regulating hacking as an investigative method was tested with regard to its (1) accessibility, (2) foreseeability, and (3) desired quality of the law.

The analysis in this chapter has shown that hacking as an investigative method is not regulated in a foreseeable manner in the Netherlands. The legal basis for this investigative method does not adequately restrict the scope of the investigative method and the examples in legislative history appear heavily outdated compared to the current state of technology and application of the investigative method in practice. Technological developments in cloud computing and 'encryption by default' of communications and devices have changed the investigative environment for law enforcement authorities. Hacking as an investigative method offers ways to overcome these challenges under the right conditions, but interferes with the right to privacy in new and intrusive manners. Therefore, hacking should be adequately regulated in order to both (1) provide law enforcement authorities with an instrument for gathering evidence in cybercrime investigations and (2) adequately protect the individuals involved.

The results of the adequacy of the Dutch regulations for this investigative method in terms of the three normative requirements are summarised in subsection 8.5.1. The specific recommendations that stem from these results are then presented in subsection 8.5.2.

8.5.1 Summary of conclusions

Section 8.1 presented an analysis of the accessibility of Dutch regulations for hacking as an investigative method. This analysis showed that detailed regulations are implemented in Dutch criminal procedural law for network

108 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 34.

searches. Based on case law and a letter from the Dutch Minister of Security and Justice, it can also be argued that an accessible legal basis is available for performing remote searches. The use of policeware can be derived from the legal basis of the special investigative power for recording private communications.

In section 8.2, the foreseeability of the Dutch legal framework for hacking as an investigative method was examined. This analysis has shown how modern investigative techniques are based on regulations that were created in the past with different applications in mind. This situation creates ambiguity with regard to the scope of the investigative methods. As a result, the foreseeability of all three types of hacking as investigative methods should be improved.

With regard to network searches, the analysis showed that the investigative method is regulated as a special investigative power in Dutch law. However, the scope of the investigative power and the manner in which the investigative power is applied are not adequately explained in the legal sources. The description of the investigative method in legislative history appears outdated and the investigative method is not even mentioned in guidelines or case law (at least in terms of its practical application). Technology has significantly progressed since the investigative power was first introduced in Dutch criminal procedural law in the early 1990s. As a result, new applications – such as accessing information that is stored in the cloud – are not only imaginable, indications in official documents are that they also take place. The Dutch legislature and Public Prosecution Service should provide clarity about the scope of the investigative method and the manner in which the method can be applied, while at the same time adequately protecting the individuals involved.

With regard to remote searches, Dutch law enforcement authorities have used an extensive interpretation of the special investigative power in art. 125i DCCP that regulates computer searches to apply remote searches. However, remote searches differ substantially from regular searches as they are applied remotely through the Internet instead of during a search in the physical world. In addition, since remote searches are applied covertly, they interfere with the right to privacy in a different – and more intrusive – manner. Dutch law enforcement authorities may therefore have overstepped their legal boundaries in basing remote searches on art. 125i DCCP. A better indication of the legal basis for this investigative method and adequate protection for the individuals involved are therefore merited in Dutch law.

With regard to the use policeware, the legal basis of the special investigative power for recording private communications applies. However, news articles indicate that functionalities of policeware have been used in practice that go beyond 'recording private communications', which creates ambiguity with regard to (1) the scope of the investigative method and (2) the manner in which policeware is now actually being used. For that reason, the investigative method is not regulated in a foreseeable manner.

Section 8.3 investigated whether the regulations for hacking as an investigative method meet the desired quality of the law. Detailed regulations and a warrant requirement were identified as an appropriate quality of the law for regulating the investigative method of network and remote searches. Currently, the applicable procedural safeguards for network and remote searches depend on where a search takes place. These regulations do not meet the desired quality of the law. Instead, the procedural safeguard of a warrant from an investigative judge should always apply. The detailed regulations and corresponding stringent procedural safeguards that apply to using the special investigative power for recording private communications meet the desired quality of the law.

8.5.2 Recommendations

Section 8.4 presented three recommendations to improve the Dutch legal framework for hacking as in investigative method. These recommendations followed the analysis of the adequacy of the Dutch legal framework based on the three normative requirements section 8.1 to 8.3. These recommendations are as follows.

1. Network searches seriously interfere with the involved individuals' right to privacy. Therefore, the existing special investigative power for network searches (art. 125j DCCP) should be amended and incorporate the requirement of a warrant from an investigative judge as a procedural safeguard.
2. A new special investigative power that enables law enforcement officials to remotely access computers as an investigative method should be created in Dutch criminal procedural law. In this context, the unique and intrusive privacy interferences that arise when this investigative method is applied merit a distinct legal basis. The proposed special investigative power for hacking as an investigative method in the Computer Crime Act III is a step in the right direction. However, the Dutch legislature should carefully scrutinise the scope of the proposed investigative power. The investigative method's current particularly broad formulation corrodes its foreseeability. Therefore, it is desirable to narrow its scope and explain the applications of this special investigative power more concretely in the explanatory memorandum and lower regulations. Furthermore, Public Prosecution Service guidelines can indicate the scope of the special investigative power and the manner in which it is applied in a concrete manner.
3. Dutch criminal procedural law should be amended to introduce a special investigative power that authorises law enforcement authorities to use policeware. As this investigative method is intrusive in terms of privacy and has many functionalities, specific provisions and appropriate procedural safeguards are justified. The proposed special investigative power for hacking as an investigate method could provide an adequate

a legal basis for this method. Due to its strict application requirements, the special investigative power meets the desired quality of the law. However, in order to meet the foreseeably requirement, a limited list of the functionalities of policeware should be provided by the legislator. The scope and the manner in which these functionalities are applied should be detailed in the explanatory memorandum. The software's functionalities should also be mentioned in both Public Prosecution Service guidelines and lower regulations concerning the use of technical devices.

Answer to research question 4

The answers to RQ4a to RQ4d in chapters 5 to 8 present an overview of the adequacy of the Dutch legal framework with regard to regulating the digital investigative methods identified in this study. As expected, the accessibility of the Dutch legal framework's regulations for these digital investigative methods did not pose major problems. The heightened criminal legality principle in Dutch criminal procedural law and the introduction of detailed regulations for special investigative methods with the Special investigative Powers Act in the late 1990s have contributed to a solid general legal basis for applying these investigative methods. However, the analyses of the two other normative requirements of foreseeability and the quality of the law produced results that are more significant. Two general observations regarding the adequacy of the Dutch legal framework vis-à-vis regulating digital investigative methods follow below.

First and foremost, *foreseeability* is lacking in relation to the regulation of digital investigative methods in the Dutch legal framework. The analyses in chapters 5 to 8 showed that Dutch law enforcement authorities have already been applying the identified investigative methods for years. However, the regulations for these investigative methods are either (1) non-existent or (2) ambiguous as to the scope and manner in which the methods are executed by law enforcement authorities. The Dutch legislature should urgently realise that evidence-gathering activities are taking place in an environment that is different from the one that existed a decade ago, when Dutch criminal procedural law was last updated to combat cybercrime. The analyses in chapters 5 to 8 have shown that the traditional investigative methods of (1) gathering open source information, (2) data production orders, (3) undercover investigations, and (4) computer searches have been transformed by the digitalisation of the environment in which law enforcement officials now conduct evidence-gathering activities. The Dutch legislature should thus move to update criminal procedural law to both (1) provide law enforcement authorities with the instruments they need to gather evidence and (2) adequately protect the individuals involved. In addition, the Public Prosecution Service has a responsibility to state the scope of and manner in which these novel investigative methods are applied in practice within (public) guidelines to contribute to a clear and foreseeable legal basis for digital investigative methods.

Second, the analyses in chapters 5 to 8 have shown that the *quality of the law* should be improved, particularly in relation to undercover investigative methods and hacking as an investigative method. The quality of the law can improved by implementing stricter procedural safeguards in the corresponding detailed regulations. The privacy interferences that accompany digital investigative methods must be interpreted in light of present-day standards (see chapter 3). As a result, the legal framework for investigative methods require amendments now, whilst the legal framework should also be continually monitored for amendments in light of new technological developments.

9 Cross-border unilateral investigations

So far, the legitimacy of the identified digital investigative methods has only been examined in the context of *domestic* applications. Chapters 5 to 8 reviewed the Dutch legal framework's (1) accessibility, (2) foreseeability, and (3) quality of the law with regard to these investigative methods. However, the Internet is global by nature and does not respect the territorial borders that legally divide our world. The borderless Internet enables cybercriminals to target victims anywhere on the planet and capitalise on jurisdictional borders by using services in States with the most favourable regulations for criminals.

In brief, the issue here is that the investigation and prosecution of cybercrime take place *locally* and are limited by the physical borders of a State, whereas cybercrimes themselves are often *cross-border* in nature (cf. Brenner & Schwerha IV 2002, p. 395). The territorial limitation of enforcement jurisdiction restricts digital evidence-gathering activities. This principle dictates that, without permission from the affected State or an authorising treaty, extraterritorial evidence-gathering activities cannot be undertaken. As a consequence, jurisdiction is a major challenge in cybercrime investigations.[1]

At the same time, the borderless Internet also enables law enforcement officials to gather evidence on foreign territory in a practical manner. When law enforcement officials do so without using mutual legal assistance requests or gaining permission from the affected State, they are undertaking a *cross-border unilateral* investigation. This application of investigative methods may enable law enforcement officials to overcome the aforementioned jurisdictional challenge. However, it still gives rise to consequences that must be further examined to assess the desirability of both applying digital investigative methods unilaterally across State borders and setting certain restrictions. In this context 'desirability' thus refers to a means for gathering evidence in a swift and practical manner that takes an activity's corresponding negative consequences into account.

This chapter explores the fifth research question with regard to the identified investigative methods that are used in cybercrime investigations (RQ 5): *To what extent is it desirable and legitimate that the identified investigative methods are applied unilaterally across State borders?* Three steps are taken to answer this question.

---

1 See section 2.5. As explained there, this study only focuses on enforcement jurisdiction. The jurisdiction to prescribe (i.e., the capacity to make and apply law) and the jurisdiction to adjudicate (i.e., the ability of national courts and other administrative bodies exercising judicial functions to hear and decide on matters) should be considered as givens.

The first step entails identifying the (legal) consequences of the cross-border unilateral application of the identified digital investigative methods. These consequences help to evaluate how the cross-border unilateral application of the identified methods should be regulated and restricted.

In the second step, a legal comparison between the Netherlands and the United States is conducted to illustrate how each State both thinks about the desirable restrictions for the cross-border unilateral application of digital investigative methods and actually regulates the identified methods.

Based on the results of the first two steps, the third step then determines the extent to which Dutch law enforcement officials can apply the identified digital investigative methods unilaterally across State borders. The aim is to pinpoint which of these methods are particularly problematic in this regard, given their consequences. The analysis identifies which investigative methods require (further) development in the international legal framework.

The structure of this chapter follows the three above-mentioned steps. Section 9.1 identifies and examines two consequences of cross-border unilateral digital investigations. In sections 9.2 to 9.5, legal comparisons between the Netherlands and the United States are conducted with regard to (1) the cross-border unilateral application of the investigative methods and (2) the legal frameworks of all four identified investigative methods.[2] Section 9.6 then determines the extent to which Dutch law enforcement officials can apply the investigative methods unilaterally across State borders. Finally, section 9.7 concludes the chapter by presenting a summary of the findings.

9.1 Consequences of cross-border unilateral investigations

Cross-border unilateral investigations are understood here as criminal investigations in which law enforcement officials physically remain in the investigating State's territory but gather evidence on foreign territory without permission from the affected State or the use of mutual legal assistance. The implications of such investigations are identified and examined in this section.

The cross-border unilateral application of investigative methods has two legal consequences that require analysis, namely (1) the infringement of the territorial sovereignty of States and (2) dangers to the legal certainty of the individuals involved in criminal investigations (in the sense that they may be subjected to the application of laws from a State other than the one in which they are located). These consequences are further analysed in subsections 9.1.1 and 9.1.2. Subsection 9.1.3 then summarises the results of the analysis.

2 This is not an exhaustive legal comparison, but a brief overview to determine which substantial differences may exist. Understanding these differences is important, as they reveal consequences that need to be taken into consideration as undesirable effects of the cross-border unilateral application of digital investigative methods.

9.1.1 Interferences with the territorial sovereignty of States

The principle of the territorial limitation of enforcement power dictates that law enforcement authorities cannot mount an investigation on foreign territory without the permission of the affected State or a basis in a treaty that authorises a particular evidence-gathering activity. As explained in subsection 2.5.1, this principle finds its origin in other principles of international law, such as (1) sovereignty, (2) the equality of States, and (3) non-intervention. The territorial restraint on criminal investigations serves first and foremost to protect the territorial sovereignty of States; it is a State's sovereign right to apply its laws and maintain security within its borders.

Ultimately, international law and the territorial limitation of enforcement power seek to ensure a stable world order (cf. Shaw 2008, p. 213 and Koops & Goodwin 2014, p. 20). Conflicts could arise between States if local law enforcement authorities were allowed to cross State borders and gather evidence on foreign territory under their own domestic laws. For that reason, mutual legal assistance functions as a mechanism that enables law enforcement authorities to collect evidence on the territory of other States. Within a mutual legal assistance treaty, a State can specify the conditions under which evidence is gathered by local law enforcement authorities (or foreign law enforcement officials under the supervision of local law enforcement authorities) upon the request of another State.[3]

Allowing a degree of cross-border unilateral evidence-gathering activities

Digital investigative methods that are commonly used in criminal investigations with regard to cybercrime enable law enforcement authorities to collect evidence across State borders, i.e., from the territory of the investigating State on the territory of another State that is affected by the evidence-gathering activity. The reactions of States to these extraterritorial activities cannot be generalised, as they are determined by the intrusiveness of the evidence-gathering activities and factors such as past grievances with the other State involved.

Gill (2013, p. 224-226 in: Ziolkowlski 2013) observes that States are likely not willing to destabilise world order and engage in armed conflict with other States over extraterritorial activities of law enforcement authorities that do not involve 'coercive' activities. Examples of coercive activities include (1) physical sabotage, (2) assassinations, and (3) abductions of individuals on another State's territory (see Gill 2013, p. 224 in: Ziolkowlski 2013). Gill argues that, for instance, extraterritorial espionage activities within the 'cyber domain' generally do not lead to an infringement of State sovereignty that rises to the level that States will engage in armed conflict

3 See further subsection 2.5.2.

(i.e., war) with each other.[4] I believe it is also unlikely that cross-border unilateral cybercrime investigations will lead to armed conflict between States. Of course, the level of power of a State and balance of power with other States also influence their responses to cross-border unilateral evidence-gathering activities (cf. Stessens 2000, p. 282).

Reactions to unilateral extraterritorial evidence-gathering activities

Nonetheless, a State can – and will – react to unilateral extraterritorial activities of law enforcement authorities that it does not deem permissible. At the very least, States can demand (a) an apology, (b) an acknowledgment of the wrongful act, and (c) a commitment to not continue those activities in the future (see Koops & Goodwin 2014, p. 75). Foreign law enforcement authorities who engage in unauthorised extraterritorial evidence-gathering activities on foreign territory can also be prosecuted under the local criminal laws of the affected State (cf. Doyle 2012, p. 22).[5] Furthermore, States can use economic and political sanctions to show their discontent with the practice. For example, the United States imposed economic sanctions on North Korea for allegedly hacking Sony Pictures Entertainment on U.S. territory.[6]

Moreover, under the reciprocity principle, States that conduct extraterritorial investigative activities can expect other States to conduct extraterritorial investigation activities on their own territory under the same circumstances. States therefore cannot allow their law enforcement officials to undertake cross-border unilateral digital investigations without expecting that law enforcement officials from other States will conduct the same activities under similar circumstances on their own territory (cf. Koops & Goodwin 2014, p. 76). In other words, the cross-border unilateral application of digital investigative methods may also have consequences for the territorial sovereignty of the investigating State itself.

---

4 It is notable that some authors argue that proportionate counterattacks are permitted in the case of economic (cyber)espionage activities. See, e.g., Messerschmidt 2013 and Skinner 2014. See also Steward Baker, Orin Kerr, and Eugene Volokh, 'The Hackback Debate', *Steptoe Cyberblog*, 2 November 2012. Available at: http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ (last visited on 29 July 2015) for an analysis of hacking back as a countermeasure in relation to criminal law in the United States and – by comparison – the report of Bert-Jaap Koops and Ronald Leenes entitled 'Acties tegen botnets door SURFnet en bij SURFnet aangesloten instellingen: strafrechtelijke aspecten' regarding criminal law aspects of counterattacks in the Netherlands. Available at: https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/expert_opinion_botnets_leenes_oktober_2013.pdf (last visited on 29 July 2015). This study does not further examine the desirability of countermeasures, since they are outside the scope of the research question.

5 See, e.g., John Leyden, 'Russians accuse FBI agent of hacking', *The Register*, 16 August 2002. Available at: http://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/ (last visited on 30 July 2015).

6 See the press release of the U.S. Department of Treasury, 'Treasury Imposes Sanctions Against the Government of The Democratic People's Republic of Korea', 2 January 2015. Available at: http://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx (last visited on 3 September 2015).

Special circumstances for extraterritorial evidence-gathering activities
In the context of the cross-border unilateral application of investigative methods on the Internet, special circumstances that make cross-border unilateral application more acceptable may arise. The reason is that in an online context, it is not always practically possible to *locate* the extraterritorial effects of the application of investigative methods. For instance, when individuals utilise the anonymising service Tor, it is practically impossible to determine the originating IP address of the network that is used to access the Internet. International law does not clearly establish how the extraterritorial effects of applying digital investigative methods should be localised and which response is appropriate to extraterritorial online evidence-gathering activities. There may be special circumstances under which certain cross-border unilateral evidence-gathering activities may be deemed acceptable – to a certain degree – by States. In this chapter, these special circumstances are identified and examined in the first subsection in sections 9.2 to 9.5.

9.1.2 Dangers to legal certainty

The principle of the territorial limitation of enforcement jurisdiction first protects the territorial sovereignty of States. However, as a corollary, individuals located within the territory of a State are protected against arbitrary interference from *foreign* law enforcement authorities in their private lives. Mutual legal assistance is the formal mechanism to gather evidence on foreign territory in criminal investigations. As Conings (2014, p. 2) points out, legal assistance mechanisms can protect citizens against interferences from foreign law enforcement officials. Mutual assistance treaties stipulate the conditions under which (usually local) law enforcement officials can gather evidence at the request of an investigating State. These conditions provide the individuals involved with legal certainty and protection to the level and conditions agreed to by the two States. It can thus be argued that State sovereignty also serves to protect citizens from external threats, including interferences with their right to privacy by foreign law enforcement officials under a different legal regime than that of the State where the citizens are located (cf. Conings 2014, p. 2).

However, a consequence of cross-border *unilateral* investigations is that legal assistance treaties are ignored, which gives rise to the question to what extent States must protect their citizens from having their lives interfered with by foreign law enforcement authorities in this manner. As explained in chapter 3, States can be held to compliance of the ECHR even outside their own sovereign territory. It can also be envisaged that a positive obligation can also be derived from the ECHR, which imposes a duty for member States to protect its citizens against interferences on their own territory – through the Internet – by foreign agents acting from other jurisdictions. In the absence of case law – to my knowledge – these latter obligations cannot be currently based on the ECHR. However, they could flow forth from broader rule of law requirements, such as those requiring legal certainty.

Individuals within the territorial borders of a State assume that their rights and freedoms are only infringed upon by *local* law enforcement authorities under the conditions stipulated in local criminal procedural law (cf. Siemerink 2000c, p. 240). People cannot be expected to know the regulations for evidence-gathering activities conducted by *foreign* law enforcement authorities. For example, law enforcement officials in State A may communicate with an individual located in State B using electronic communication services facilitated by the Internet in an online undercover investigation. In such a case, the individual involved is subjected to governmental power that is applied by foreign law enforcement authorities. When foreign law enforcement officials apply their own domestic regulations, these regulations cannot be accessible and foreseeable to the individual involved. These foreign officials' use of enforcement power can thus endanger *legal certainty* – and ultimately the rule of law, because the practice leads to an arbitrary interference of governmental authorities in the private lives of the individuals involved (cf. De Smet 1999, p. 144).

9.1.3 Section conclusion

The analyses in subsections 9.1.1 and 9.1.2 have shown that cross-border unilateral investigations (1) interfere with the territorial sovereignty of the affected State and (2) endanger the legal certainty of the individuals involved.

To determine the severity of the interference with the territorial sovereignty of States when investigative methods are unilaterally applied across State borders, it is necessary to consider the intrusiveness of the investigative methods being utilised. States view the intrusiveness of investigative methods and thereby also gravity of the interference with the territorial sovereignty of a State differently when that investigative method is applied extraterritorially. Sections 9.2 to 9.5 therefore present a legal comparison that is conducted to examine how States perceive the intrusiveness of the extraterritorial application of digital investigate methods in terms of territorial sovereignty and the right to privacy of the individuals involved. The legal comparison is conducted between the Netherlands and the United States.[7] The possible existence of special circumstances that may serve as the basis for States deeming that the cross-border unilateral application of certain investigative methods is more acceptable is also explored.

To determine the dangers to legal certainty caused by cross-border unilateral investigations, it is necessary to examine how the regulations of digital investigative methods differ between States and evaluate the extent to which those differences are a threat to legal certainty. In order to explore the similarities and differences in the regulation of digital investigative methods, sections 9.2 to 9.5 also present a legal comparison of these regulations between the Netherlands and the United States.

7 See subsection 1.4.2 for the underlying reasons why these two States were selected.

9.2 The gathering of publicly available online information

This section examines the consequences of the cross-border unilateral gathering of publicly available online information. In subsection 9.2.1, a legal comparison is conducted of how the Netherlands and the United States view the extent to which the cross-border unilateral application of this investigative method interferes with the territorial sovereignty of States. To examine the dangers to the legal certainty of the individuals involved, subsection 9.2.2 presents a legal comparison of the manner in which the two States regulate the investigative method. A section conclusion is then provided in subsection 9.2.3.

9.2.1 Interferences with territorial sovereignty

When law enforcement authorities gather publicly available online information, they copy information from webservers and other computers all over the world. For that reason, one can argue that this type of information gathering produces extraterritorial effects.

A 'computer-orientated jurisdiction principle' is traditionally used to localise a digital investigative method. This principle focuses on the location of a computer to determine the effects of a digital investigative method (cf. Conings & Oerlemans 2013, p. 27). For example, the location of a computer that is remotely accessed by law enforcement authorities pinpoints where the extraterritorial effects of an investigative method take place.

The gathering of publicly available online information can thus interfere with the territorial sovereignty of the State in which the data is located. As a result, that investigation activity can – theoretically – not be applied given the territorial sovereignty of the affected State, unless (1) permission is obtained from the affected State or (2) a legal basis that authorises the evidence-gathering activity is available in a treaty.

Treaty basis for the evidence-gathering activity

The Convention on Cybercrime, which was ratified in Budapest in 2001, explicitly provides a treaty basis for the cross-border unilateral application of this investigative method. The treaty basis is provided in art. 32(a) of the convention, which reads as follows:

"A party may, without the authorisation of another Party: (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically".

Member States of the Convention on Cybercrime thus agree that cross-border unilateral access to publicly available data – which is technically stored in computers that may be located on foreign territory – is permitted, without

the need for legal assistance to acquire the evidence.[8] In other words, the States that have ratified this convention agree that the evidence-gathering activity does not interfere with their territorial sovereignty (cf. Koops 2013, p. 658). As the Netherlands and the United States have both ratified the Convention on Cybercrime,[9] their respective law enforcement officials can access publicly available information stored in computers on each other's territory.

It may be argued that the cross-border unilateral collection of publicly available online data that is stored in a computer on the foreign territory of a State that has not ratified the convention is not allowed without permission and may violate the territorial sovereignty of the affected State (see Koops 2011, p. 43-44). However, this approach would ignore the fact that the cross-border unilateral gathering of publicly available online information has been tacitly tolerated by States for almost two decades (cf. Seitz 2005, p. 38). To my knowledge, no State has either formally asked other States for permission to access publicly available information on the Internet or formally objected to the practice. Seitz (2005, p. 38) submits that the cross-border unilateral application of this investigative method is allowed under *international customary law*. However, customary international law is only created when States or a group of States behave openly in a certain manner because they understand that such behaviour is permitted under international law (Koops & Goodwin 2014, p. 20). In addition, it is required that other States do not object to the practice. Indeed, States have tacitly tolerated the cross-border unilateral gathering of publicly available online information for almost two decades and no State has formally objected to the practice. In addition, the convention's Ad-hoc Subgroup on Transborder Access and Jurisdiction declared in 2013 that:

"transborder access to publicly available data (Article 32(a)) may be considered accepted international practice and part of international customary law even beyond the Parties to the Budapest Convention".[10]

The Council of Europe understands '*transborder access*' as unilateral access to computer data stored on another State's territory without that State's consent (see TC-Y 2014, p. 6). At the same time however, States may not be aware of the evidence-gathering activity on their territory. For example, if a Dutch citizen is active in dealing drugs on an online black market, law enforcement officials can observe the behaviours of that black market's member as part of their domestic criminal investigation. Since most cybercriminals use nicknames on online forums, it is difficult to know which

8 See the explanatory memorandum Convention on Cybercrime, par 293.

9 The Netherlands ratified the convention on 16 November 2006. The United States ratified it on 29 October 2006. See http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (last visited on 24 March 2016).

10 T-CY 2013, p. 10.

States are experiencing the territorial effects of the evidence-gathering activity. In these cases, it is problematic to object to the practice.

Nevertheless, the interference with the territorial sovereignty of other States that takes place when this investigative method is unilaterally applied across State borders appears to be minor in nature. The Convention on Cybercrimes allows for the evidence-gathering activity and States have tacitly tolerated the cross-border unilateral gathering of publicly available online information for almost two decades. The cross-border unilateral gathering of publicly available online information is therefore considered acceptable in this study.

9.2.2 Dangers to legal certainty

The fact that the cross-border unilateral application of this method is accepted does not mean that legal certainty is not endangered. When law enforcement officials apply domestic laws that regulate their investigative methods and these investigative methods affect the rights and freedoms of an individual located on foreign territory, the regulations relating to these methods are not accessible or foreseeable for the individual involved. As such, his legal certainty is endangered. States regulate the gathering of publicly available online information in different manners, as illustrated in this subsection using a brief comparison of the Dutch and U.S. regulations concerning this investigative method.

The Dutch legal framework for the gathering of publicly available online information has already been examined extensively in chapter 5. A summary of the results of that analysis is provided below under A. A brief analysis of the U.S. (federal) regulations for this investigative method is presented under B. Finally, the most important differences between the two sets of regulations are identified under C, to illustrate how the cross-border unilateral application of this investigative method can endanger the legal certainty of the individuals involved.

A Overview of Dutch regulations

In the Netherlands, both the manual and automated gathering of publicly available online information are currently only restricted by data protection regulations. In chapter 5, it was argued that more detailed regulations and a more foreseeable legal framework are required for both of these investigative methods, as data protection regulations are not tailored to them and do not adequately indicate the scope of the methods or the manner in which they are applied in practice. For the manual gathering of publicly available online information, a Public Prosecution Service guideline may suffice. However, it was argued that detailed regulations in statutory law should be created tor the automated gathering of publicly available online information, given that this investigative method is regarded as more privacy intrusive.

The online observation of individuals is regulated in detail as a special investigative power in the Netherlands, insofar as the investigative method is applied systematically. To create a more foreseeable legal framework for this method, it was recommended that guidelines clarify when online observation becomes systematic and hence when the special investigative power is applicable. In the Netherlands, observation is in itself regarded as an investigative method that interferes with the right to privacy of the individual involved.

B Overview of U.S. regulations

The U.S. Supreme Court has made it clear that certain constitutional rights related to the first ten amendments to the U.S. Constitution (i.e., the Bill of Rights) also apply to the evidence-gathering activities of U.S. law enforcement authorities (LaFave et al. 2009b, p. 2). The Fourth Amendment to the U.S. Constitution, which bars the U.S. government from conducting unreasonable searches and seizures in relation to U.S. citizens, is of particular importance to the investigative methods discussed in this study. It should be emphasised that this amendment only protects certain elements of the right to privacy as detailed in art. 8 ECHR. Unlike the Netherlands, the United States does not have a general constitutional 'right to privacy'.

The Fourth Amendment in relation to the investigative method is examined in B.1. Thereafter, whether (federal[11]) regulations of criminal procedures restrict the investigative method at hand is considered in B.2. The (internal) guidelines of U.S. law enforcement authorities that may restrict the investigative method are examined in B.3 (insofar as they are publicly available).

B.1 Fourth Amendment to the U.S. Constitution

The Fourth Amendment reads as follows:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

A textual approach to the Fourth Amendment suggests that searches and seizures are limited to the seizure of physical objects during a search at a physical place. However, the constitutional protection provided by this amendment is broader. The decision in *Katz v. United States* played an important role in broadening its scope.[12]

11 The analysis in this chapter is restricted to U.S. criminal procedural law on a federal level. U.S. states also have the jurisdiction to regulate investigative methods.

12 U.S. Supreme Court 18 December 1967, *Katz v. United States*, 389 U.S. at 347-351 (1967).

In the landmark case of *Katz v. United States* in 1967, the U.S. Supreme Court decided that a warrantless microphone recording of a telephone conversation conducted within a public phone booth was unconstitutional given that it violated the Fourth Amendment.[13] The U.S. Supreme Court thereby decided that the Fourth Amendment not only protects U.S. citizens against a physical search with regard to tangible objects, but also vis-à-vis *intangible* 'objects'.[14] In this case, the intangible object was the telephone conversation held inside a telephone booth. The *Katz* judgement created the possibility that other (digital) investigative methods also fall within the scope of the Fourth Amendment.

The case of *Katz v. United States* is also important, because the '*reasonable expectation of privacy*' doctrine was developed in its decision. In his concurring opinion, justice Harlan developed the test to determine whether a person has a reasonable expectation of privacy. This test has two requirements: (1) the individual must demonstrate a subjective expectation of privacy in relation to the object and (2) this privacy expectation must be one that (U.S.) society recognises as reasonable.[15] After all, the Fourth Amendment only protects citizens against *unreasonable* searches. In the context of gathering publicly available information on the Internet, the following quote from the *Katz v. United States* case is relevant:

"What a person knowingly exposes to the public, (…) is not a subject of Fourth Amendment protection."[16]

Interpreted in an online context, this means that U.S. citizens do not have a reasonable expectation of privacy when they knowingly disclose information on publicly accessible parts of the Internet. The protection of the Fourth Amendment does not apply in this situation (cf. DoJ Manual 2009, p. 5, Kerr 2010, p. 447 and Brenner 2010, p. 194). The above quote in *Katz v. The United States* is clearly referred to in the 2002 case of *U.S. v. Gines-Perez*, in which the judge stated that it is:

"obvious that a claim to privacy is unavailable to someone who places information on an indisputably public medium such as the Internet, without taking any measures to protect that information."[17]

13 U.S. Supreme Court 18 December 1967, *Katz v. United States*, 389 U.S. at 347-351 (1967).

14 Citing the case of U.S. Supreme Court 6 March 1961, *Silverman v. United States*, 365 U.S. at 511 (1961).

15 U.S. Supreme Court 18 December 1967, *Katz v. United States*, 389 U.S. at 361 (1967) (J. Harlan, concurring). Kerr convincingly argues that – in practice – the 'reasonable expectation of privacy test' only consists of one test: whether an individual's expectation of privacy is one that U.S. society recognises as reasonable (Kerr 2014).

16 U.S. Supreme Court 18 December 1967, *Katz v. United States*, 389 U.S. at 351-352 (1967).

17 The U.S. District Court District of Puerto Rico, *United States v. Gines-Perez*, 214 F. Supp. 2d 205, at 225 (2002).

However, publicly available online information is not necessarily disclosed by the individual himself. As such, one can argue that the reasonable expectation of privacy doctrine does not apply when one's personal information is published by others. Yet, another exception to the Fourth Amendment warrant requirement, called the '*public vantage doctrine*', may apply in that situation. The public vantage doctrine means that U.S. law enforcement officials are "*entitled to see anything that any member of the public could see from a similar series of vantage points*" (Stuntz 1995, p. 1022-1023). The cases of *California v. Ciraolo*[18] and *Florida v. Riley*[19] were influential in developing this doctrine (see Petrashek 2009, p. 1523-1524). In the case of *California v. Ciraolo*, U.S. law enforcement officials investigated a report of marijuana growth in the backyard of an individual. They decided to fly a small airplane over the (fenced-in) backyard of the individual to determine whether marijuana plants were indeed present. The suspect objected to this investigative activity and argued that a warrant was required to conduct this search. The U.S. Supreme Court disagreed and concluded that Fourth Amendment was not violated.[20] In *Florida v. Riley*, U.S. law enforcement officials used a helicopter to observe what was located in a partially covered greenhouse in the backyard of a residence. The suspect contended a warrant was required for the investigative activity. Again, the U.S. Supreme Court disagreed and concluded the Fourth Amendment was not violated (and thus no warrant was required for the aerial observation).[21]

Petrashek (2009, p. 1525) explains how the public vantage doctrine is important in the context of the gathering of publicly available online information. The authors cites several cases in which U.S. courts decided that individuals have no reasonable expectation of privacy in the publishing of information on publicly accessible social media websites, chatrooms, and online discussion forums.[22] The reason that these individuals have no reasonable expectation of privacy is that the online information is accessible by anyone. A U.S. federal guideline for a 'Developing a Policy on the Use of

18 U.S. Supreme Court 19 May 1986, *California v. Ciraolo*, 476 US 207 (1986).
19 U.S. Supreme Court 23 January 1989, *Florida v. Riley*, 488 U.S. 445 (1989).
20 U.S. Supreme Court 19 May 1986, *California v. Ciraolo*, 476 US at 215 (1986).
21 U.S. Supreme Court 23 January 1989, *Florida v. Riley*, 488 U.S. at 451 (1989).
22 Citing the cases of U.S. Court of Appeal of California (5th District), *Moreno v. Sentinel, Inc.*, 2 April 2009, no. F054138 (2009), in which the U.S. court stated *"Here, Cynthia publicized her opinions about Coalinga by posting the Ode on myspace.com, a hugely popular internet site. Cynthia's affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material"*, U.S. Court of Appeals for the Armed Forces, 21 November 1996, *United States v. Maxwell*, no. 95-0751 (1996), in which the U.S. court stated: *"Messages sent to the public at large in the 'chat room' or e-mail that is 'forwarded' from correspondent to correspondent lose any semblance of privacy"*, and U.S. Court of Appeals (6th Circuit), 2 July 2001, *Guest v. Leis*, 255 F.3d 325 (2001), in which the U.S. court decided that U.S. law enforcement officials can assume undercover identifies, access an online discussion forum and download images, because "*users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting*".

Social Media in Intelligence and Investigative Activities' confirms that it is part of 'normal law enforcement activity' (based on the law enforcement purpose) to search a suspect's Facebook page that is publicly accessible (cf. Global Justice Information Sharing Initiative 2013, p. 14).[23] The guideline confirms that the evidence gathering activity does not require a warrant. The guideline suggests that only a 'minimal' authorisation level should be required by law enforcement authorities for the manual gathering of publicly available online information (cf. Global Justice Information Sharing Initiative 2013, p. 14).

B.2 U.S. criminal procedural law

The U.S. Congress also influenced criminal procedure law in the United States by establishing the Federal Rules of Criminal Procedure in Title 18 of the U.S. Code. The U.S. Congress may enact legislation governing both federal and state criminal justice systems. However, it has used this authority only sparingly (see LaFave et al. 2009a, p. 18).[24] No federal criminal procedure regulations address the gathering of publicly available online information.

B.3 Guidelines for U.S. law enforcement authorities

U.S. law enforcement authorities are also bound by (internal) guidelines in their evidence-gathering activities. In the United States, individuals involved in criminal investigations cannot derive rights from these guidelines.[25] As a result, these guidelines have a different status than the regulations and guidelines that were discussed in relation to the legal framework in the Netherlands, where citizens can derive rights from these public guidelines. Furthermore, the policies may vary for each U.S. law enforcement authority, both on a local and federal level. However, these guidelines do provide information about how the investigative methods are restricted in practice. Therefore, the relevant aspects are examined below.

The FBI Domestic Investigations and Operations Guide 2011 provides indications about applicable internal regulations. More specifically, the guideline defines publicly available information as follows*:*

23 The guideline explains on p. 13 that a valid law enforcement purpose means that a law enforcement official can, for example, search for and access an individual's Facebook profile to identify an alleged criminal, but not look for information on a new neighbour.

24 Note that U.S. states are sovereign and can also prescribe laws and enforce that code through the agencies and procedures that it creates (see LaFave et al. 2009b, p. 2). Each of the 50 U.S. states has the authority to create criminal procedural law. In addition to these 50 states, (1) the District of Columbia (no. 51) (i.e., the Washington D.C. area) has the power to prescribe and enforce its own laws and (2) the U.S. Congress (no. 52) has created a criminal justice system of its own to enforce the general criminal code by federal agencies in federal courts (see LaFave et al. 2009b, p. 3).

25 See, e.g., the FBI Domestic Investigations and Operations Guide 2011, part 2-10, section 2.5.

"public information is 'Publicly Available Information' that is:
(A) Published or broadcast for public consumption;
(B) Available on request to the public;
(C) Accessible on-line or other to the public;
(D) Available to the public by subscription or purchase;
(E) Made available at a meeting open to the public;
(F) Obtained by visiting any place or attending an event that is open to the public (e.g., public places); or
(G) Observed, heard, smelled, detected or obtained by any casual observer or member of the public and does not involve unconsented intrusion in private places".[26]

Furthermore, the FBI guideline clarifies that U.S. law enforcement officials can (manually) gather publicly available online information without 'supervisory approval'.[27] Unfortunately, the '*On-Line Investigations*' appendix to the internal guideline of the FBI is regarded as classified and is thus not available for analysis.[28] It therefore remains uncertain whether specific regulations apply to the gathering of publicly available online information by the FBI.[29]

With regard to the automated gathering of publicly available online information, no specifics are provided in the FBI guideline. However, the guideline of the U.S. Georgia Bureau of Investigation Investigative Division developed a specific policy for the use of 'social media monitoring tools' (which is a type of automated data collection system).[30] The provisions in the guideline provide an illustration of how the investigative method may be regulated in the internal guideline of a U.S. law authority. The procedure is as follows. Authorisation of the 'Deputy Director of Investigations' is required to use social media monitoring tools in criminal investigations. The request for authorisation must specify: (1) a description of the social media monitoring tool; (2) its purpose and intended use; (3) the social media websites the tool will access; (4) whether the tool is accessing information in the public domain or information protected by privacy settings; and (5) whether information will be retained by the law enforcement authority and if so, the applicable retention period of such information. If approved, the tool may

26 See FBI Domestic Investigations and Operations Guide 2011, part 18-7, section 18.5.1.1.
27 See 18.5.1.3. The article also states that the rule does not apply when a law enforcement official attends a religious service, even in public.
28 FBI Domestic Investigations and Operations Guide 2011, part L-1.
29 In is noteworthy that in the U.S. federal 'Guideline for Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities' puts special emphasis on articulating a policy to determine the accuracy, validity, and/or authenticity of the information that is obtained from social media sites. The validation is important, since the information is often uploaded by users and a wrong classification may lead to privacy violations or inappropriate actions (see, e.g., Global Justice Information Sharing Initiative 2013, p. 15-16). This is indeed important for the gathering of publicly available online information as an investigative method. However, these regulations do not regard the regulation of the investigative method itself. Therefore, they are not further examined in this study.
30 See appendix I of the Global Justice Information Sharing Initiative 2013, p. 32.

be used for 90 days. After 90 days, a summary of the results of the use of the social media monitoring tool must be provided. It is reiterated here it is important to realise that the existence of this single provision in an internal guideline for a local U.S. law enforcement authority does not mean that all U.S. law enforcement currently use this model guideline; its policies to use automated online data collection systems may vary considerably.

The definition of publicly available information in the guideline for domestic FBI investigations indicates that the *online observation* of the behaviours of individuals is also understood as 'gathering publicly available information'.[31] Therefore, the same regulations apply for the online observation of online behaviours of individuals as for the manual gathering of publicly available online information.

Once the information is gathered and processed by U.S. law enforcement officials, data protection guidelines are applicable for the storage of information in the 'criminal intelligence systems' of U.S. law enforcement authorities (cf. Global Justice Information Sharing Initiative 2013, p. 12). The Criminal Intelligence Systems Operation policy, which is part of the Code of Federal Regulations, is the guiding regulation for the storage of information in a criminal intelligence system in the United States (Carter 2009, p. 149). As the specifics of data protection regulations are not of interest to the research question, they are not further examined.

C Notable differences in approach

Regulations related to the gathering of publicly available information are essentially similar in the Netherlands and the United States. Criminal procedural law does not regulate the (manual and automated) gathering of publicly available online information in detail in either State. Data protection regulations pertain to the investigative method, but they are not applied in a concrete manner – which leaves ambiguity with regard to the scope of the investigative method and the manner in which the investigative method is applied.

In the Netherlands, the investigative method is regarded as an activity that interferes with the right to privacy, albeit not in a particularly serious manner. It was suggested that more detailed regulations be created in statutory law for the automated gathering of publicly available online information. A special investigative power restricts the investigative method of the systematic observation of online behaviours.

In the United States, a general right to privacy does not exist in the U.S. Consitution. The investigative method is not restricted by the Fourth Amendment. As such, the warrant requirement does not apply to the investigative method. Furthermore, this method is not restricted by regulations in federal criminal procedural law. Internal guidelines may or may not restrict the investigative method for U.S. law enforcement authorities. However,

31 See FBI Domestic Investigations and Operations Guide 2011, part 18-7, section 18.5.1.1.

individuals cannot derive any rights from these guidelines. In general, it appears that the investigative method is not regarded as particularly an intrusive investigative method and does not require authorisation. One guideline for a local U.S. law enforcement authority indicates that authorisation of a deputy director is required to make use of automated online data collection systems. The examined guidelines do not distinguish between (1) the manual gathering of publicly available online information and (2) the observation of the individuals' online behaviours; instead, they appear to treat everything as the 'gathering of publicly available information'. This can be explained by the U.S. approach that individuals do not have reasonable expectation of privacy in information that is publicly available to anyone, including by use of observation as an investigative method.

Based on the results of the analysis, it is apparent that accessible and foreseeable regulations for the investigative method do not exist in the United States. The situation is not particularly different in Dutch law. However, an important difference is that in Dutch law, detailed regulations in criminal procedural law apply to the observation of individuals' online behaviours. Namely, a special investigative power that requires authorisation from a public prosecutor is required when the investigative method is applied 'systematically'. In contrast, online observation as an investigative method is not restricted by either a warrant requirement or federal criminal procedure rules in the United States. It appears the investigative method is treated as gathering publicly available information as an investigative method, which requires no special authorisation for law enforcement officials to conduct.

9.2.3 Section conclusion

The analysis in this section has shown that the Convention on Cybercrime provides a treaty basis for the cross-border unilateral gathering of publicly available online information. Both the Netherlands and the United States have ratified the convention and agreed that cross-border unilateral evidence-gathering activities do not infringe their territorial sovereignty. In addition, it is argued that the cross-border unilateral application of the investigative method can be regarded as part of customary law. The interferences with other States' territorial sovereignty when the investigative method is unilaterally applied across State borders also appear to be limited. Therefore, it is not likely that States will object to the practice. As a result, mutual legal assistance is not required to obtain evidence through the cross-border unilateral application of this method.

However, the analysis in subsection 9.2.2 has also shown that the legal certainty of Dutch citizens can be endangered when U.S. law enforcement officials systematically observe their behaviours in an online context. All actors in the criminal justice system should be aware that States regulate this investigative method in different manners and the gathering of publicly available online information (including observation) is not restricted to State borders.

9.3 Data production orders

This section examines the consequences of the cross-border unilateral issuing of data production orders to online service providers. Subsection 9.3.1 explores how the Netherlands and the United States each view the desirable restrictions of the cross-border unilateral application of this investigative method. Section 9.3.2 then compares how both States have regulated the investigative method, in order to identify the regulatory differences that illustrate the dangers to legal certainty. A section conclusion is provided in subsection 9.3.3.

9.3.1 Interferences with territorial sovereignty

States in continental Europe, including the Netherlands, generally regard unilateral data production orders that are issued to companies on foreign territory as a violation of the affected State's territorial sovereignty (cf. Stessens 2000, p. 329, Ryngaert 2008, p. 81 and Gercke 2012, p. 277). To obtain information from online service providers that are located abroad using data production orders, Dutch law enforcement authorities thus require permission of the State in which that company is located or a treaty basis that authorises their evidence-gathering activity.

However, State practice reveals a different picture. The reality is that hundreds of millions of individuals utilise online services that are provided by U.S. companies. A complex ICT infrastructure that makes use of cloud computing techniques in data centres located throughout the world supports these services and enables them to be provided to individuals regardless of where they live. Dutch law enforcement authorities require the cooperation of these companies in order to obtain data using data production orders.

Based on the theoretical framework provided above, Dutch law enforcement authorities need permission from the United States or use mutual legal assistance, each time they send a data production order to a U.S. company. Like any other EU State, the Netherlands can be party to both bilateral treaties with other States and multilateral treaties that are created by the Council of Europe or European Commission. This has led to a situation in which many – and a wide variety of – mutual legal assistance treaties are applicable in the Netherlands.[32] Of these treaties, only the Convention on Cybercrime potentially provides a treaty basis to unilaterally issue data production orders to an online service provider on foreign territory.

32 The texts of these treaties are publicly accessible at: https://verdragenbank.overheid.nl/nl (last visited on 30 September 2015).

Treaty provisions in the Convention on Cybercrime?

Art. 32(b) of the Convention on Cybercrime potentially provides a treaty basis for the unilateral issuance of data production orders to foreign online service providers. It reads as follows:

"A Party may, without the authorisation of another Party: (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

This provision may enable law enforcement officials to issue a (domestic) data production order to a company on foreign territory, which can in turn *voluntarily* comply with it (cf. Walden 2011, p. 8, Koops et al. 2012b, p. 37 and UNODC 2013, p. 219).

However, the provision would then assign *companies* the power to decide whether information should be disclosed to law enforcement authorities, whereas *States* have traditionally decided which investigational activities can take place on their territory (cf. Gercke 2012, p. 277). This is why certain States still view companies' voluntary disclosure of information to foreign law enforcement authorities as a violation of their territorial sovereignty (see Koops et al. 2012b, p. 37).[33] Another difficulty is that national laws can limit the voluntary disclosure of data. Most notably, the voluntary disclosure of data to law enforcement authorities may violate data protection regulations.[34]

In 2014, the Working Group of the Convention on Cybercrime on Transborder Access to Computer Systems provided clarity and explicitly stated in its report that art. 32(b) of the Convention on Cybercrime *does not* provide a legal basis for the cross-border unilateral issuance of data production orders to online service providers (TC-Y 2014, p. 7).[35] This convention thus does not provide a treaty basis for issuing data production orders unilaterally

33 Referring to PC-OC (2009) 05, p. 6 and PC-OC (2008) 01, p. 28).

34 See, e.g., the 'Article 29 Working Party's comments on the issue by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime', letter to the Council of Europe, 5 December 2013, p. 3. Koops and Goodwin (2014, p. 45) also point out that data protection law prescribes that only transfers of personal information is only allowed outside the European Economic Area, insofar as the foreign State has an 'adequate level of data protection'. In that respect, it is noteworthy that the Safe Harbour decision (2000/520/EG) for data transfers from EU Member States to the United States has recently been declared invalid (CJEU 6 October 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner)*. In response, new legislation called 'Privacy Shield' was created to replace the Safe Harbour agreement in 2016.

35 The working group also makes it clear that the terms and conditions of an online service do not constitute explicit consent to disclose information on a voluntarily basis to law enforcement authorities, even if these terms and conditions indicate that data may be shared with criminal justice authorities in cases of abuse (see TC-Y 2014, p. 7).

to online service providers located in foreign territory, who can then disclose information voluntarily, although it does specify that such a practice is not necessarily a violation of international law.[36] Ultimately, the convention does not provide clarity on the matter.

State practice

Even though art. 32b of the Convention on Cybercrime does not formally provide a treaty basis for issuing cross-border unilateral data production orders to online service providers, it appears that in practice, online service providers do *voluntarily* disclose information to law enforcement authorities.[37] For example, based on the company's own policy statement, Microsoft voluntarily discloses information to non-U.S. law enforcement authorities. It states on its website that it allows for the voluntary disclosure of *non-content data* to non-U.S. law enforcement authorities *"in response to a valid legal request"* (…) that is *"validated locally and transmitted to our compliance teams."*[38] These 'valid legal requests' must comply with the local laws of the requesting authority, as authenticated by a local team or law firm in the requesting State.[39]

Microsoft's policy thus indicates that it voluntarily discloses non-content data, i.e. (1) subscriber data, (2) traffic data, and (3) other data, to foreign law enforcement authorities under the local laws of the investigating State after a review by local law firm and Microsoft's compliance team. As a consequence, non-U.S. law enforcement authorities can only obtain content data with a U.S. warrant and mutual legal assistance.[40] Microsoft's transparency reports show that the company has not disclosed any content data to Dutch law enforcement authorities in the past, although it has disclosed subscriber and other data.[41]

The territorial effects of data production orders are traditionally determined by the location of the data that is disclosed to law enforcement authorities. Following this line of reasoning, the State in which data is located dictates the terms concerning how information is disclosed to law

36 See TC-Y 2014, p. 6.

37 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 9.

38 Available at: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/ (last visited on 30 July 2015). Emphasis added by the author.

39 See http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/ (last visited on 30 July 2015).

40 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 9-10. For a different viewpoint, see Odinot et al. (2013, p. 40) and Koops et al. (2012, p. 20 and p. 38-40), who indicate that Dutch law enforcement authorities reportedly have to use mutual legal assistance procedures to obtain data from U.S. online service providers. It seems to depend on the service provider and the type of information whether information is voluntarily disclosed to law enforcement authorities.

41 Available at: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ (last visited on 30 July 2015).

enforcement authorities (as part of its sovereign rights). Spoenle (2010, p. 4-5) points out that due to cloud computing techniques, the location of data can no longer reasonably determined. Due to cloud computing techniques, data can continuously move between servers. This is called the 'loss of knowledge of location' problem for law enforcement authorities (see Koops & Goodwin 2014, p. 48). When the location of data cannot be ascertained, it is difficult to determine a data production order's extraterritorial effects.

However, taking account the practice of the voluntarily disclosure of data described above, it appears that it is more likely that the location of the online service provider that controls the information determines which regulations apply (cf. UNODC 2013, p. 216). The online service provider can extract the data being sought from its servers in different locations around the world and send it to law enforcement authorities. It can be argued that, as the online service providers are located in a certain State, the online service provider must meet local regulations, including those that specify how data should be disclosed to law enforcement authorities.

Unilateral data production orders and the Dutch approach

The practice in which online service providers decide themselves whether to voluntarily disclose information may still lead to results that are unsatisfying to law enforcement authorities. This is illustrated by the following Dutch case. In 2012, an unknown individual impersonated a Dutch student and published discriminatory statements in that student's name on Twitter. These statements damaged the reputation of the student, who subsequently sought help from Dutch law enforcement authorities. These authorities can obtain subscriber data from an online service provider such as Twitter. As explained in subsection 2.2.1, an IP address may provide the information required to identify an internet user. When Twitter refused to disclose the information voluntarily, Dutch authorities submitted a legal assistance request to U.S. authorities. However, they did not receive the information because the discriminatory statements were not illegal in the United States. In response to parliamentary questions concerning the case, the Dutch Minister of Security and Justice provided the above facts but took no further action.[42]

In 2011, Belgian law enforcement authorities decided to take a different approach and unilaterally applied a data production order that was regulated in Belgian criminal procedural law in order to obtain data relating to the online service provider Yahoo! Inc.[43] The data production order was sent, because Yahoo! Inc. refused to cooperate and (voluntarily) disclose the information following the data production order. The Belgian courts were greatly divided as to whether the unilateral application of Belgian law was

42 See also J.J. Oerlemans, 'Antwoord Kamervragen over identiteitsfraude VU-studente', *Computerrecht* 2014, no. 1, p. 57-58.

43 For an extensive analysis of the cases, see, e.g., De Hert & Boulet 2012, De Schepper & Verbruggen 2013, Kerkhofs & Van Linthout 2013, and Verbuggen 2014.

allowed in this instance.[44] The judges eventually reasoned that since Yahoo! Inc. offers its services to Belgian citizens, the company is 'located' in Belgium and Belgian law enforcement authorities have jurisdiction to apply local law. The Belgian courts subsequently fined Yahoo! Inc. for not cooperating with the legal order to disclose customer information to Belgian law enforcement authorities under Belgian law.[45]

De Schepper and Verbruggen (2013, p. 161) point out that the Belgian courts essentially ignored the difference between jurisdiction to prescribe and jurisdiction to enforce in international criminal law. Although Belgian law enforcement authorities may be authorised to prescribe their laws to Yahoo! Inc., they are not allowed to *enforce* their criminal procedural laws on foreign companies by imposing fines for non-compliance with Belgian law (cf. Verbruggen 2014, p. 137). The principle of the territorial restriction of enforcement power does not allow States to enforce their laws on foreign territory. It is also questionable whether the fine imposed on Yahoo! Inc. can be enforced in practice. As Yahoo! Inc. does not have any assets or employees in Belgium, the Belgian State does not have the option to use force against persons or companies on its territory to enforce local law (cf. De Schepper & Verbruggen 2013, p. 164). Additionally, foreign courts do not enforce the decisions of another State's criminal court without consent from the competent State authorities. There is thus almost no chance that U.S. courts will fine Yahoo! Inc. in the United States to uphold the Belgian decision to fine the company.

In comparison to Belgium, the Netherlands appears to adopt a more moderate approach. In practice, Dutch law enforcement authorities issue data production orders to foreign online service providers, who then decide whether to voluntarily disclose the requested information. If they opt not to, the authorities will turn to mutual legal assistance. The Dutch legislature emphasises that these procedures 'take a considerable amount of time'.[46] As far as I am able to determine through my research, Dutch law enforcement officials have not issued unilateral data production orders to online service providers. It is also clear that no online service providers were sanctioned by Dutch courts for not disclosing information to Dutch law enforcement authorities.

---

44 See Court of First Instance Dendermonde, 2 March 2009, *Tijdschrift voor Strafrecht* 2009, no. 2, p. 117-120; Court of Appeal Gent, 30 June 2010, *Computerrecht* 2010, no. 6, p. 351; Belgium Supreme Court, 18 January 2011, *AM* 2011, no. 2, p. 218 m. nt. Vandezande; Court of Appeal Brussels, 12 October 2011, *AM* 2012, no. 2-3, p. 238 m. nt. De Schepper, Belgium Supreme Court 4 September 2012, *Digital Evidence and Electronic Signature Law Review* 2013, 10, p. 155-157 m. nt. Vandendriessche; Court of Appeals Antwerpen, 20 November 2013, *Tijdschrift voor Strafrecht* 2014, no. 1, p. 75-76 m. nt. Schoorens.

45 See K. De Schepper, 'Doek valt over Yahoo-zaak', Computerrecht 2016, no. 1, p. 76.

46 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 8-0.

U.S. approach

The United States has a different view on the territorial limits of enforcement jurisdiction when it comes to issuing data production to companies on foreign territory. This State's law enforcement authorities are known for sending data production orders to foreign companies in the event that cooperation through legal assistance is not likely to secure the information they need (cf. Snow 2002, p. 231).

This approach originated in the 1980s, when U.S. law enforcement officials issued data production orders to banks that had local branches or conducted business in the United States and law enforcement officials needed documents that had to be obtained from a branch of these banks on foreign territory.[47] In these cases in the 1980s, U.S. courts determined that:

"the U.S. interest in investigating crime is greater than the foreign interest in bank secrecy and that banks must comply with the subpoenas regardless of the potential hardship they may suffer due to the conflict with foreign law" (Snow 2002, p. 232).

This practice of U.S. courts, which entails conducting a 'balancing of interests' test to decide whether unilateral data production orders are allowed, is rather peculiar from the strict European continental viewpoint on the territorial limitation of enforcement jurisdiction (cf. Maier 1983, p. 584).[48] Scholars from continental Europe generally view this practice as a violation of international law, as it violates both the foreign State's sovereignty and the principle of non-intervention (cf. Ryngaert 2008, p. 80-81). The compelled production of documents stored on foreign territory is viewed as an act of enforcement power that requires consent or a treaty basis for execution (cf. Gercke 2012, p. 277).

The same U.S. practice of unilateral data production orders also currently occurs when data production orders are issued to online service providers. For example, in 2014 Microsoft fought a data production order that U.S. law enforcement authorities sent under U.S. law to obtain stored content data on servers at Microsoft's subsidiary in Ireland.[49] Microsoft had already handed over subscriber data and traffic data to U.S. law enforcement authorities, but it refused to execute the data production order with regard to content data. Microsoft was of the opinion that the information being sought should have been obtained using mutual legal assistance conditions as stipulated in Irish law, stating that Irish law and EU directives apply to

47 See most notably the Nova Scotia cases, U.S. Court of Appeals, 11th Circuit Court 29 November 1982, In re Grand Jury Proceedings (*Bank of Nova Scotia I*), 691 F.2d 1384 (1982) and U.S. Court of Appeals, 11th Circuit Court 14 August 1984, In re Grand Jury Proceedings Bank of Nova Scotia (*Bank of Nova Scotia II*), 740 F.2d 817 (1984).

48 See, e.g., Mann: *"It is difficult to imagine a clearer case in which American legal chauvinism has led to the disregard of elementary rules of international law"* (Mann 1984, p. 52).

49 See Brad Smith, 'We're Fighting the Feds Over Your Email', *The Wall Street Journal* (opinion), 29 July 2014. Available at: http://www.wsj.com/articles/brad-smith-were-fighting-the-feds-over-your-email-1406674616 (last visited on 2 February 2015).

"Hotmail and Outlook.com accounts hosted in Ireland".[50] The U.S. Department of Justice argued that under the Stored Communication Act, the location of the records is irrelevant. The appropriate test for the production of the information is *control of the information*, not the location of the information. In this case, Microsoft employees in the United States could access the data in the United States without the involvement of Irish authorities (see Schwerha IV 2015, p. 10-11). In the first instance of the case, Microsoft was ordered to hand the data stored in Ireland over to U.S. law enforcement authorities. The U.S. court held that the investigative activities took place in the United States when U.S. law enforcement officials reviewed the data. The U.S. also court determined that the relevant question was whether the data was in Microsoft's control. As it was, the information had to be disclosed based on the data production order.[51] In appeal, the U.S. Court of Appeals (2nd Circuit) disagreed and concluded that the Stored Communications Act does not have an extraterritorial reach.[52] The content data is located on servers of a data centre of Microsoft in Ireland. Therefore, using the location of the stored data as a localisation principle, the judges concluded that a U.S. warrant under the Stored Communications Act cannot force Microsoft to send the data from Ireland to the United States.[53] Interestingly, in his concurring opinion, judge Lynch warned that the judgment leads to the dangerous conclusion that the privacy protection of individuals is now in the hands of companies that can simply relocate their infrastructure to avoid complying with the Stored Communication Act.[54] For that reason, he urged that – should the Stored Communications Act be revised – the international reach of the statute should be clarified and balanced against het interests of other sovereign States.[55] The U.S. Department of Justice can go in appeal to the judgment. I expect that when the Stored Communications Act is amended by the U.S. Congress, the statute will be given explicit extraterritorial reach

50 Available at: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/ (last visited on 20 March 2014).

51 See U.S. District Court Southern District of New York, *In re Warrant to Search a Certain E-Mail account Controlled and Maintained by Microsoft Corp*., 25 April 2014, F.Supp.3d 466. See also David Kravets, 'Microsoft ordered to give US customer e-mails stored abroad', *Ars Technica,* 31 July 2014. Available at: http://arstechnica.com/tech-policy/2014/07/microsoft-ordered-to-give-us-customer-e-mails-stored-abroad/ (last visited on 16 January 2015).

52 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Microsoft Corporation v. United States of America, 14 July 2016, p. 42.

53 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Microsoft Corporation v. United States of America, 14 July 2016, p. 39.

54 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Microsoft Corporation v. United States of America, 14 July 2016, conc. J. Lynch, p. 4.

55 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Microsoft Corporation v. United States of America, 14 July 2016, conc. J. Lynch, p. 20.

in order to enable U.S. law enforcement authorities to acquire data from U.S. companies under U.S. regulations. Such a policy will also suit the (Third) Restatement on Foreign Relations Law of the United States, which clearly provides for the possibility that a U.S. company can be compelled to hand data over to U.S. law enforcement authorities, even when that data is stored on foreign territory.[56]

In its *Transborder Access and Jurisdiction* report, the Transborder Group of the Cybercrime Convention Committee of the Council of Europe also affirmed that the United States is of the opinion that it can "*request data from any cloud server located anywhere around the world*", insofar as these online service providers are subject to U.S. jurisdiction.[57] According to the report, U.S. law enforcement authorities assume that an online service provider is subject to U.S. jurisdiction when that entity (1) is based in the United States, (2) has a subsidiary or office in the United States, or (3) otherwise conducts continuous and systematic business in the United States.[58] Based on the report and the abovementioned Restatement it is likely that U.S. will maintain the practice of serving unilateral data production orders if necessary, even when the data is located on foreign territory (cf. De Schepper & Verbruggen 2013, p. 162).[59]

9.3.2 Dangers to legal certainty

This subsection illustrates the dangers to legal certainty that arise when law enforcement officials issue data production orders to foreign online service providers using a brief comparison of relevant Dutch and U.S. regulations.

The Dutch legal framework for data production orders that are issued to online service providers has already been extensively examined in chapter 5. A summary of the results is presented under A below. A brief analysis of the U.S. (federal) regulations for this investigative method is conducted under B. Finally, the most important differences between the two sets of regulations are identified under C.

56 See Restatement (Third) of Foreign Relations Law § 442(1)(a): *"A court of agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, object, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States"* (emphasis added by the author). 'A person' is in practice interpreted as a company that falls under U.S. jurisdiction, even if that company also has an establishment abroad.

57 T-CY 2012, p. 48.

58 T-CY 2012, p. 48.

59 See also Kruijsen 2013, who refers to the U.S. Court of Appeals, 9th Circuit Court, 3 October 2011, *Suzlon Energy, Ltd. v. Microsoft Corporation* (2011), 671 F.3d 726, in which the 9th Circuit Court ordered Microsoft to hand information from an Indian account holder over.

A Overview of Dutch regulations

In the Netherlands, data production orders are regulated by a bipartite legal regime that stipulates in detail the conditions under which (1) electronic communication service providers and (2) all (other) persons, institutions, and companies must disclose information to law enforcement authorities. These authorities can gather the following categories of data using data production orders: (1) subscriber data, (2) traffic data, (3) other data, (4) sensitive data, and (5) content data.[60]

The procedural safeguards that apply to data production orders (i.e., authorisation from a law enforcement official, public prosecutor, or investigative judge) depend on the gravity of the privacy interference that the orders cause. Data production orders that gather subscriber information are regarded as the least intrusive and law enforcement officials are not required to obtain authorisation from a higher authority. Data production orders that gather content data are seen as the most intrusive and require a warrant from an investigative judge.[61] In section 6.3 of chapter 6, stronger procedural requirements were proposed for data production orders in the categories of other data and traffic data in the Netherlands.[62]

B Overview of U.S. regulations

The U.S. regulations for data production orders that are issued to online service providers are examined in B.1, by analysing the Fourth Amendment in relation to the investigative method. The detailed regulations for this investigative method in U.S. criminal procedural law are then explored under B.2.[63]

B.1 Fourth Amendment to the U.S. Constitution

The U.S. Supreme Court has held in several judgments that when information has been 'revealed to a third party' by a citizen, the Fourth Amendment to the U.S. Constitution is not violated if that information is then disclosed by the third party to law enforcement authorities. Any subjective expectation of the involved individual that third parties will keep the information confidential is not relevant (DoJ Manual 2009, p. 8). This exception to the warrant requirement for searching for evidence at a particular place is called the '*third party doctrine*'. The landmark cases of *United States v. Miller*[64] and

60 See section 6.1 of chapter 6.

61 These are visualised in Figure 6.1 in the introduction to chapter 6.

62 See chapter 6 for a more extensive overview.

63 The manual for Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations of the U.S. Department of Justice (DoJ Manual 2009) is also referred to when it provides additional relevant information.

64 U.S. Supreme Court 21 April 1976, *United States v. Miller*, 425 U.S. 435, at 443-444 (1976). In the case of *United States v. Miller*, the U.S. Supreme Court held that the Fourth Amendment does not protect bank account information, because an account holder must assume the risk that the information in control of the third party is conveyed to the government.

Smith v. Maryland[65] established the general rule that when information is in the hands of third parties, an individual lacks a reasonable expectation of privacy with regard to disclosure of that information (Solove 2004, p. 201). Internet service providers are also considered third parties. Lower U.S. courts have confirmed that U.S. citizens have no reasonable expectation of privacy concerning subscriber information that is stored at online service providers (cf. Petrashek 2009, p. 1522).[66]

However, lower courts have recently held that the constitutional protection of the Fourth Amendment does apply to '*stored content information*' that is available at third parties. In the United States, content data is understood as *"any information concerning the substance, purport, or meaning of that communication"*.[67] Most notably, in the case of *Warshak v. the United States*, the U.S. 6th Circuit Court of Appeals decided that the contents of e-mail are protected by the Fourth Amendment.[68] Other (lower) courts subsequently decided that Fourth Amendment protection also applies to other stored content at online service providers, for instance Facebook messages (cf. Kerr 2013, p. 6).[69] Federal legislation has been proposed in the United States, which would require law enforcement officials to obtain a warrant to acquire content data from online service providers by the use of data production orders.[70]

B.2 U.S. criminal procedural law

In 1986, the U.S. Congress created the Stored Communications Act (hereinafter: SCA) to protect personal data that is available at communication

65 U.S. Supreme Court 20 June 1979, *Smith v. Maryland*, 442 U.S. 735, at 743-744 (1979). In the case of *Smith v. Maryland*, the court also held that individuals have no reasonable expectation of privacy in phone numbers dialled by the owner of a telephone, because the act of dialling a number effectively discloses that information to the phone company.

66 See, e.g., U.S. District Court for Connecticut 9 August 2005, *Freedman v. America Online*, 325 F. Supp. 2d 638 (2005) (obtaining subscriber data from the internet access provider AOL): *"In the cases in which the issue has been considered, courts have universally found that, for purposes of the Fourth Amendment, a subscriber does not maintain a reasonable expectation of privacy with respect to his subscriber information"*, U.S. Court of Appeals (10th Circuit) 11 March 2008, *United States v. Perrine*, 518 F.3d 1196, at 1204 (2008) (obtaining subscriber data from Yahoo! Inc with regard to its webmail service and the internet access provider Cox Communications), U.S. Illinois Southern District Court 11 April 2009, *Courtright v. Madigan et al.* (2009) (obtaining subscriber data from social media service MySpace).

67 See 18 U.S.C. § 2510(8).

68 U.S. Court of Appeals (6th Circuit) 14 December 2010, *Warshak v. United States,* 490 F.3d 455 at 266 (2010). Unfortunately for the suspect, the evidence was admissible because the officers relied on good faith on the provisions of the SCA.

69 See, e.g., U.S. District Court of Minnesota, 6 September 2012, *R.S. and S.S. v. Minnewaska Area School*, Dist. No. 2149, F. Supp.2d, p. 29 (2012).

70 See April Glasier, 'It May Soon Be a Lot Harder for the Law to Get Into Your Email', *Wired*, 29 April 2016. Available at: https://www.wired.com/2016/04/finally-might-verge-email-privacy-reform/ (last visited on 24 May 2016).

service providers (cf. Kerr 2004, p. 1212).[71] The SCA regulates the mandatory disclosure of information upon orders from U.S. law enforcement authorities or judges.[72] Under the SCA, U.S. law enforcement officials can use the following three instruments to obtain data: (1) a subpoena, (2) a d-order, and (3) a warrant.

A 'subpoena' is a legal order that compels a third party to disclose data (cf. Kerr 2010, p. 516).[73] The requirements for issuing a subpoena are low (DoJ Manual 2009, p. 128-133). The government must show that the information it seeks is *"relevant to the investigation"* and its production not *"overly burdensome"* (Stuntz 1995, p. 1038).[74]

A 'd-order' derives its name from the legal article on which it is based, namely 18 U.S.C. § 2703(d). This court order specifies the conditions under which online service providers are compelled to disclose information to law enforcement authorities. A d-order can be issued by any federal magistrate from a district court or an equivalent judge from a state court at the request of law enforcement officials.[75] Kerr (2010, p. 514) describes the requirements for obtaining a d-order as "*something of mixture of a subpoena and a search warrant*". Law enforcement officials must provide *"specific and articulable facts showing that there are reasonable grounds to believe"* that the information to be compelled is *"relevant and material to an ongoing criminal investigation."*[76]

A search warrant is a judicial order authorising police to execute a search or seizure under stringent legal thresholds (Kerr 2010, p. 289). Search warrants are only provided by a magistrate judge at request of a law enforcement official. The two conditions to obtain a warrant are (1) 'probable cause' and (2) the particularity requirement. Probable cause means that *"a fair prob-*

---

71 The SCA is part of the broader Electronic Communications Privacy Act of 1986 (hereinafter: ECPA). The ECPA is codified in U.S. federal criminal procedural law in 18 U.S.C. §§ 2701-12.

72 In the United States, information can also be voluntarily disclosed in case (1) the disclosure is made with the lawful consent of the customer or subscriber (which can possibly be derived from terms and conditions), (2) the provider believes in good faith that an emergency involving the danger of death or serious physical injury requires the disclosure without delay, and (3) the disclosure is made to the National Center for Missing and Exploited Children, for instance when child pornography is discovered on a service provider's network (see 18 U.S.C. par 2702(b) and 18 U.S.C. par 2702(c)).

73 With regard to subpoenas, see further LaFave 2009a, p. 7-8 and LaFave 2009b, p. 10. With more extensive regard to grand jury subpoenas, see LaFave 2009a, p. 435-511. The United States also grants a limited subpoena authority to federal law enforcement agencies for the investigation of particular crimes (LaFave 2009a, p. 8). These subpoenas are called 'administrative subpoenas'. For example, the FBI has an administrative subpoena authority in the investigation of drug-related crimes and child abuse cases.

74 Stuntz remarks that courts measure the relevance and burden with a *"heavy thumb on the government's side of the scales"* (Stuntz 1995, p. 1038).

75 See for example 18 U.S.C. §§ 2703(d) and 2711(3).

76 See 18 U.S.C. §§ 2703(d) . The 'specific and articulable facts' standard derives from the U.S. Supreme Court's decision in U.S. Supreme Court 10 June 1968, *Terry v. Ohio*, 392 U.S. 1 (1968), p. 21. See also U.S. Court of Appeals (10th Circuit) 11 March 2008, *United States v. Perrine*, 518 F.3d 1196, at 1202 (2008).

ability exists that contraband or evidence of a crime will be found in a particular place" (DoJ Manual 2009, p. 64).[77] In the context of digital evidence, the particularity requirement means that law enforcement officials must describe which information is being sought where. A warrant should describe how to separate relevant from irrelevant items. In addition, the evidence that is looked for must be limited to the scope of the probable cause established in the search warrant (DoJ Manual 2009, p. 69-70).

The categories of data production orders that can be issued to online service providers (as distinguished in this study) are further examined below.[78]

Subscriber and traffic data

The SCA specifies that a subpoena can be issued to enable U.S. law enforcement officials to obtain both subscriber and traffic data from online service providers. The scope of the data production order is restricted by a limited list of data.[79] The following data can be obtained from a subscriber under this legal basis: (a) name, (b) address, (c) records of session times and durations of a communication, (d) length of service (including start data) and types of services, (e) other subscriber number or identity (such as an IP address), and (f) means of payment for such service. This is reflected in policies of online service providers, such as Google, that state on their website how they handle data production orders that are send to them by law enforcement authorities.

For example, Google states on its website that with regard to its webmail service Gmail, law enforcement officials can request the following information with a valid subpoena: (1) subscriber registration information (e.g., name, account creation information, associated e-mail addresses, phone number) and (2) sign-in IP addresses and associated time stamps.[80]

Other data

In the United States, law enforcement officials can obtain other data – i.e., data that does not fall into the subscriber, traffic, or content categories – from online service providers using a d-order. To make this category of data more

77 The standard has been defined *"as where the facts and circumstances within the officer's knowledge are sufficient in themselves to warrant a person of reasonable prudence to belief that contraband or evidence of a crime will be found in a particular place or on a particular person"* (U.S. Supreme Court 2 March 1925, *Carroll v. United States*, 267 U.S. 132, at 162 (1925).

78 In the United States, there is also ambiguity with regard to exactly which SCA regulations apply to online service providers, as the legal orders are differentiated between 'electronic communication service providers' and 'remote storage providers'. For readability, only the term 'online service providers' is used. This simplifies the U.S. legal framework to some extent. However, the essence of the regulations and their accompanying procedural safeguards remains unchanged.

79 See 18 U.S.C. § 2703(c)(2).

80 See https://www.google.com/transparencyreport/userdatarequests/legalprocess (last visited on 30 April 2016).

concrete an example is given. Google states on their website that the company provides following information under a valid d-order:

"a government agency can obtain the same information as a subpoena, plus more detailed information about the use of the account. This could include the IP address associated with a particular email sent from that account or used to change the account password (with dates and times), and the non-content portion of email headers such as the "from," "to" and "date" fields. An ECPA court order is available only for criminal investigations."[81]

Content data

The category of content data is ill defined in U.S. law. Kerr (2004, p. 1228) explains that the SCA refers to the U.S. Wiretap Act for the definition of content information. However, that definition "only states what it includes, not what it actually is" (Kerr 2004, p. 1228). The Wiretap Act specifies that content information 'includes any information concerning the substance, purport, or meaning of communications'.[82] Content data involves electronically stored communications and clearly includes e-mails that are available at online service providers, but it remains unclear what other data is considered content data (cf. Kerr 2013). In this respect, it is notable that online service providers such as Google already state on their websites that they require a warrant not just for e-mail, but also for "search query information" and "private content stored in a Google Account, such as Gmail messages, documents, photos and YouTube videos".[83]

The U.S. regulations for obtaining content data from online service providers are particularly complex.[84] For the purposes of this study and comparison, it is most important to note that e-mails that are more than 180 days old can be obtained with either a subpoena or d-order,[85] while a SCA warrant is required for e-mails that are 180 days old or less.[86]

When a warrant is executed under the SCA, *"all e-mails from within an email account"* are handed over to the investigators *"who then identify and copy information that fall within the scope of the particularized 'items to be seized' under the warrant"* (DoJ Manual 2009, p. 134).[87] It is debatable whether the

81 See https://www.google.com/transparencyreport/userdatarequests/legalprocess/ (last visited on 30 April 2016).

82 See 18 U.S.C. § 2510(8).

83 See https://www.google.com/transparencyreport/userdatarequests/legalprocess/ (last visited on 30 April 2016).

84 For an extensive analysis, see, e.g., Kerr 2004 and Kerr 2010.

85 See 18 U.S.C. § 2703(b)(1)(b)(i) and 18 U.S.C. §2703(b)(1)(b)(ii).

86 See 18 U.S.C. §2703(a)

87 See also Brid-Aine Parnell, 'US judge: YES, cops or feds SO CAN SLURP an ENTIRE Gmail account', *The Register*, 21 July 2014. Available at: http://www.theregister.co.uk/2014/07/21/judge_okays_cops_slurping_entire_email_account/ (last visited on 21 July 2014). The is called a '2703-warrant', derived from its legal basis in 18 U.S.C. § 2703.

disclosure of an entire e-mail account meets the 'particularity requirement' of a warrant.

As explained above, there is a trend in case law that content data available at third parties can only be collected with a warrant. In addition, congressional legislation that would amend the SCA to require a warrant for content data has been proposed.

C Notable differences

From a fundamental rights perspective, the most notable difference between Dutch and U.S. law in the context of data production orders is that individuals in the Netherlands are protected by the right to privacy as articulated in art. 8 ECHR when online service providers disclose data that they store to law enforcement officials. In the United States, individuals are not protected by the warrant requirement of the Fourth Amendment for information that is available at online service providers, due to the third party doctrine. Lower U.S. courts have however recently provided Fourth Amendment protection to content data stored at online service providers, although the scope of what content data entails and the protection that it is currently provided in practice remain unclear.

Nevertheless, the regulations for using data production orders to obtain data from online service providers are essentially similar in the Netherlands and the United States. The criminal procedural laws in both States contain detailed regulations that protect personal information from individuals that is stored at online service providers. In addition, both States differentiate data production orders on the basis of the orders' sensitivity. This is done in a similar manner, although more types of data production orders are regulated in detail as investigative powers in the Netherlands. In addition, it is clear that in the Netherlands, stored e-mails available at an online service provider can only be obtained with a warrant.

However, these similar regulations are not identical and differences can still endanger the legal certainty of the individuals involved. For example, Google states on its website that it can voluntarily disclose information to non-U.S. law enforcement authorities "*if those requests are consistent with international norms, U.S. law, Google's policies and the law of the requesting country.*"[88] However, exactly what "Google's policies" entail is not public.[89] For instance, what if Brazilian law enforcement authorities request data from U.S. online service providers concerning an individual located on Dutch territory? Will information be disclosed based on Brazilian criminal

88 Available at: https://www.google.com/transparencyreport/userdatarequests/legalprocess/ (last visited on 30 July 2015).

89 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 9: *"The transparency reports by companies such as Google and Microsoft provide insufficient information about the willingness of companies to cooperate [by voluntarily disclosing data to Dutch law enforcement officials] and do not specify the origin and legal basis [of data production orders]."*

procedural law, Dutch criminal procedural law, or U.S. criminal procedural law? Online service providers may experience a conflict of regulations in this situation.

Practice also shows that U.S. law enforcement authorities send data production orders unilaterally across State borders to online service providers to obtain data that is located outside U.S. territory. The legal certainty of individuals is endangered when that data belongs to individuals who do not reside in the United States. At the same time, individuals should – in my view – realise that when they make use of U.S. online services, U.S. law enforcement authorities can obtain their information under U.S. law.[90] The practice of issuing cross-border unilateral data production orders to online service providers becomes especially problematic in terms of both State sovereignty and legal certainty, when data production orders are issued to online service providers that are located on foreign territory (as well as their infrastructure).

9.3.3 Section conclusion

Online service providers can potentially offer their services to individuals who are located all over the world. At the moment, U.S. online services are particularly popular. Non-U.S. law enforcement authorities, including Dutch law enforcement authorities, want to be able to gather evidence that is located at these online service providers. A practice has emerged in which online service providers voluntarily disclose information to foreign law enforcement authorities after receiving data production orders, even when that information is potentially physically located in a data centre on foreign territory.

Dutch law enforcement authorities follow this practice. There are no indications that they unilaterally issue data production orders across State borders and force these providers to disclosure data under the threat of a fine if they do not cooperate. Foreign online service providers decide themselves whether to disclose data voluntarily. If the data is not voluntarily disclosed, mutual legal assistance procedures must be used to gather the data. Online service providers may experience conflicting obligations caused by regulations, when foreign law enforcement officials issue a data production order or the data relates to an individual that is located on foreign territory. In this situation, the legal certainty of the individual involved is also endangered.

---

90 After the latest Microsoft Ireland decision (U.S. Court of Appeals District Court of Connecticut (2nd Circuit) 14 July 2016, *Microsoft Corporation v. United States of America* (In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation), this is only true for non-content information. However, in my view it is likely the decision will be overturned by a different U.S. Court or the SCA will be amended to allow for an extraterritorial application. This belief is founded by the examined previous case law with regard to bank records and the policy formulated in the Restatement (Third) of Foreign Relations Law.

U.S. law enforcement authorities do send data production orders unilaterally across State borders to online service providers that potentially store their data on foreign territory. This practice is understandable for U.S. online service providers. These online service providers are regulated by the United States. The cross-border unilateral issuance of data production orders to foreign companies that only provide services to U.S. residents, without assets in the United States, is more problematic in terms of both State sovereignty and legal certainty.

No treaty basis is available for either the voluntarily or mandatory disclosure of information by online service providers after the cross-border unilateral issuance of data production orders. It can therefore be argued that this practice is in violation of international law. However, the practice can be explained by the popularity and large growth of online services in the last decade, which has led to law enforcement authorities wanting to obtain data from these online service providers in an efficient manner. The practice endangers the legal certainty of the individuals involved, since it is unclear under which conditions – and even which laws – online service providers disclose information to foreign law enforcement authorities.

9.4 Online undercover investigations

The section examines the consequences of cross-border unilateral undercover investigations. Section 9.4.1 explores what the Netherlands and the United States think about desirable restrictions for the cross-border unilateral application of the investigative method. Section 9.4.2 then compares how the two States have regulated this method to identify the regulatory differences that illustrate the dangers to legal certainty. A section conclusion is provided in subsection 9.4.3.

9.4.1 Interferences with territorial sovereignty

The territorial limitation of enforcement jurisdiction leads to the restriction that investigative methods can only be applied within the borders of State, insofar as no permission is obtained from the other State and no treaty basis that authorises the evidence-gathering activity is available. Brownlie describes this principle as follows:

"Persons may not be arrested, a summons may not be served, police or tax investigations may not be mounted, orders for production of documents may not be executed, except under the consent of a treaty or other consent given" (Crawford 2012, p. 479).

The Netherlands is of the opinion that this territorial limitation of enforcement jurisdiction also applies to undercover investigative methods. The use of investigative methods to gather evidence in criminal cases is not allowed

outside of Dutch territory without permission from the involved State(s) or a legal basis in a treaty (cf. Klip 1995, p. 1057).[91] Vice versa, only Dutch law enforcement officials are entitled to use investigative methods on Dutch soil in order to gather evidence in criminal investigations (cf. Klip 1995, p. 1066). The use of investigative methods includes undercover investigative methods, which are regulated in detail in Dutch criminal procedural law. For that reason, the Netherlands did not approve the extraterritorial undercover operations conducted by U.S. Drug Enforcement Administration (DEA) agents on Dutch territory in the 1980s and 1990s (cf. Klip 1995, p. 1068, Van der Wilt 2000 p. 176, and Koers 2001, p. 399).[92] It regarded the extraterritorial evidence-gathering activities of U.S. law enforcement officials in the physical world as a violation of Dutch territorial sovereignty. The Netherlands considers undercover investigative methods as an intrusive investigative method, but not as intrusive as a search at a place or computer hacking.[93]

The Internet makes it particularly straightforward to apply undercover investigative methods across State borders. The Internet enables a law enforcement official to interact with an individual who can be located anywhere in the world. Law enforcement officials no longer have to physically cross State borders to conduct an extraterritorial undercover operation. The extraterritorial effects of online undercover operations must be localised based on where the affected individual resides. Following the territorial restriction of enforcement jurisdiction, it can be argued that permission must be obtained from the State where the individual is located or a relevant treaty basis must be available for the cross-border unilateral evidence-gathering activity (cf. Siemerink 2000a, p. 69).

---

91 See *Kamerstukken II* (Parliamentary Series Second Chamber) 1990/91, 22 142, no. 3, p. 10. While referring to art. 539a DCCP, the legislature at the time explained that the use of *"penal enforcement power outside a State's territory is only allowed with consent of the foreign State"* (translated from Dutch). See also, *Kamerstukken II* (Parliamentary Series Second Chamber) 1985/86, 19 328, no. 1, p. 3: *"It is unacceptable when foreign informants operate outside the supervision of (Dutch) law enforcement authorities on Dutch territory"* (translated from Dutch). This statement is repeated in *Kamerstukken II* (Parliamentary Series Second Chamber) 1990/91, 21800VI, no. 39, p. 16. See also Rb. Amsterdam, 27 April 2007, ECLI:NL:RBAMS:2007:BA4017. See for a more recent example, answers to questions of parliamentary member Nispen regarding an U.S. undercover operation in the Netherlands, 4 July 2016, no. 2016Z11467: *"The mutual legal assistance treaty between the United States and the Netherlands prescribes that mutual legal assistance is required to conduct investigative activities on each other's territory"* and "*It is a well-known principle in international law that law enforcement officials are not allowed to conduct investigative activities on another State's territory without permission"* (translated by the author).

92 See answers to questions of parliamentary member De Wit regarding foreign law enforcement authorities, 19 March 2007, no. 5474459/07. The Dutch Minister of Security and Justice at the time formally protested to his U.S. counterpart about the unilateral operation of the DEA on Dutch territory in 2007 (see Rb. Amsterdam, 27 April 2007, ECLI:NL:RBAMS:2007:BA4017). The minister also made arrangements with the DEA to prevent such behaviour in the future.

93 See the analysis in chapter 7 and 8 regarding the regulation of these investigative methods in the Netherlands.

It is expected that the Netherlands views the cross-border unilateral application of online undercover investigative methods that involve foreign individuals as acceptable only insofar as permission is obtained from the affected State or a treaty basis that authorises the evidence-gathering activity is available. When a treaty regulates the application of undercover investigative methods on the territory of a different State in the physical world, the relevant treaty provision also applies to the online application of undercover investigative methods.

However, circumstances may exist in which the cross-border unilateral application of online undercover investigative methods that involve foreign individuals is acceptable from a Dutch (and continental) law perspective. When the individual involved in a criminal investigation uses a nickname and an IP address is not available as a (usable) digital lead (for example because these individuals are utilising Tor or other anonymising services), the extraterritorial effects of the undercover operation cannot be localised. In this situation, the principle of the territorial application of enforcement power cannot be applied. As a result, it can be argued that cross-border unilateral online undercover investigative operations are acceptable when the location of the individuals involved cannot be reasonably determined (cf. O'Floinn & Ormerod 2011). For example, in a U.S. undercover operation conducted by the DEA, U.S. law enforcement officials reportedly bought drugs that was offered by on an advertisement by an individual with the nickname 'adamsflower' on the website 'pharmacyrater.com'. This evidence-gathering activity constitutes a pseudo-purchase in the Netherlands, which requires the application of the special investigative power of a pseudo-purchase that can be authorised by a public prosecutor for the investigation of crimes defined in art. 67 DCCP. Eventually, the suspect was traced down to his residence in the Netherlands by U.S. law enforcement authorities and arrested by Dutch law enforcement authorities upon request. He was extradited to the United States in 2014. After almost two years, he was returned to the Netherlands to serve the remainder of his sentence.[94] The case led to controversy in the Netherlands, because U.S. law enforcement authorities were accused of conducting an undercover operation in the Netherlands without permission of the Dutch State and using an illegitimate form of entrapment for the online pseudo-purchase. The Dutch Minister of Security and Justice stated in response to parliamentary questions that U.S. law enforcement officials can conduct an online pseudo-purchase of drugs that are offered by 'a global anonymous online crime organisation', even when it becomes clear *after* the operation that the individual that sold the drugs was located on Dutch ter-

94 See Tom Kreling & Huib Modderkolk, 'De dealer die in de Amerikaanse val werd gelokt', *De Volkskrant*, 7 June 2016. The journalists state (based on court documents) that U.S. law enforcement authorities already knew the suspects location, since subscriber data and e-mails were obtained from the Canadian webmail service 'Hushmail'. The Dutch suspect may have also been identifiable by subscriber data and traffic data available at the online payment service PayPal and the money transmitting service Western Union.

ritory.[95] The Dutch Minister also (rightfully) explained that with regard to the pseudo-purchase no entrapment had taken place, since the goods were already offered on a website by the suspect. As will be further explained in subsection 9.4.2, the concept of entrapment in the Netherlands and United States differ. Therefore, the application of online pseudo-purchase could be problematic when law enforcement officials have many interactions with the suspect prior to the pseudo-purchase. The undercover operation does raise the question to which extent these operations can take place and at which point in the investigation law enforcement officials must attempt to localise the suspects. For example, law enforcement officials can attempt to localise individuals by sending data production orders to obtain subscriber data from online services that the involved individuals utilise. As soon as the location of the individual is known, mutual legal assistance should be used to conduct evidence-gathering activities with extraterritorial effects on foreign territory.

In addition, different investigative methods may interfere with State sovereignty at different levels of severity. In chapter 7, online undercover investigative methods were distinguished as (1) online pseudo-purchases, (2) online interactions with individuals, and (3) online infiltration operations. When online pseudo-purchases and online infiltration operations are applied, undercover agents commit authorised crimes. These investigative methods may be regarded as a violation of the affected State's territorial sovereignty when no permission is provided by the affected State to conduct the (often minor) crime on its territory (cf. O'Floinn & Ormerod 2011). Online interactions with individuals may be regarded as less intrusive investigative methods, since they only involve law enforcement officials interacting with individuals in an undercover capacity. States may find this type of online undercover operations (in which no crimes are committed) being undertaken on their territory without their permission as more acceptable. Interestingly, the individuals involved may regard these online interactions as more privacy intrusive than, for example, online pseudo-purchases by law enforcement officials.

However, no formal policy is available that indicates how Dutch law enforcement authorities take the territorial restriction of enforcement jurisdiction into consideration in the context of undercover investigative methods. Based on the Dutch interpretation of the territorial restriction of undercover operations in the physical world, it follows that online undercover investigations are also restricted to the territory of the Netherlands.

95 See answers to questions of parliamentary member Nispen regarding an U.S. undercover operation in the Netherlands, 4 July 2016, no. 2016Z11467. Confusingly, the Minister of Security and Justice also stated that 'no investigative activities took place on Dutch territory'. In my view, evidence-gathering activities factually did take place on Dutch territory. However, it is possible that in first instance, no permission of the Dutch State could be obtained since the location of the individual involved was unclear. The minister informs Dutch parliament that mutual legal assistance has been obtained by U.S. law enforcement officials for the application of other investigative methods.

The territorial effects of the investigative method can be localised using an individual's location. Unless, of course, his location cannot be reasonably determined. It is conceivable that in this situation it is possible to apply online undercover investigative methods unilaterally across State borders, as is also supported by the above mentioned examined letter send to Dutch Parliament.

U.S. approach

Historically, U.S. law enforcement authorities have been more willing than other States to gather evidence across their own State borders by applying cross-border unilateral undercover investigations. Nadelmann (1993, p. 472) aptly describes the U.S. attitude as follows:

"Among the features that distinguish US international law enforcement behavior from that of most other states, however, are the relatively high number of endeavors in which US officials act unilaterally and coercively. No other government has acted so aggressively in collecting evidence from foreign jurisdictions, apprehending fugitives from abroad, indicting foreign officials in its own courts, targeting foreign government corruption, and persuading foreign governments to change their criminal justice norms to better accord with its own."

Indeed, the United States appears to have a view on the territorial restrictions of undercover investigation activities that differs from views held by other States, including the Netherlands.[96] In particular with regard to undercover investigative methods, a possible explanation for the willingness of the United States to conduct undercover operations on foreign territory is that U.S. law enforcement authorities do not view undercover operations as privacy-infringing activities.[97] The analysis in subsection 9.4.2 below further examines the differences between U.S. and Dutch regulations in relation to undercover investigative methods.

The questions are of course whether U.S. law enforcement authorities still conduct undercover operations on foreign territory and whether this practice is continued in an online context. The United States has greatly increased its number of mutual legal assistance treaties with other States since the 1980s. These treaties should facilitate extraterritorial evidence-gathering activities, including undercover operations, which are undertaken by local law enforcement authorities in the physical world (cf. Snow 2002, p. 211). As argued above, these treaties should be interpreted similarly in an online context. However, it may occur that the extraterritorial effects of undercover operations cannot be localised and thus States cannot be not

96 See also Klip 1995, p. 1068, Hoffer 2000, Van der Wilt 2000, p. 176 and Koers 2001, p. 399.

97 Koers (2001, p. 400) points to the one-sided and perhaps hypocritical approach of the United States regarding these unilateral extraterritorial investigation measures, since article 18 U.S.C. § 951 dictates that foreign law enforcement officials are not authorised to conduct investigations on U.S. territory under sanction of a prison sentence.

asked for permission. It is also possible that a different localisation method is used or that individual law enforcement officials simply overstep their boundaries and engage in extraterritorial undercover evidence-gathering activities without consulting on their actions with the appropriate authorities.

The case of David Schrooten illustrates how an online undercover operation can take place in practice.[98] This case also illustrates how these operations can produce extraterritorial effects that potentially interfere with the territorial sovereignty of a State (here the Netherlands) and clearly interfere with the legal certainty of the individual involved. The case is further examined below.

The U.S. Secret Service suspected David Schrooten, a Dutch national, of credit card fraud that involved U.S. victims.[99] At trial, Schrooten's defence counsel stated that the Secret Service had assumed the online identity of a suspect who had been apprehended in the United States and had subsequently used his online account to interact with Schrooten (who was in the Netherlands) in an undercover capacity via the Internet.[100] As explained under C in subsection 2.2.2, the power of law enforcement officials to take over a person's online identity is a unique feature of online undercover operations. The Secret Service agents then purchased credit card numbers from Schrooten, who used the nickname 'Fortezza' on the Internet. Thereby, an online pseudo-purchase as an investigative method was conducted, which requires the application of a special investigative power in the Netherlands by local law enforcement officials or permission of the Dutch State to conduct the online pseudo-purchase. The U.S. law enforcement officials maintained contact with David Schrooten. At one point in the investigation, the suspect flew to Romania to visit his girlfriend. When he arrived, Schrooten was arrested at the airport by Romanian authorities and extradited to the United States. Schrooten was ultimately incarcerated in a U.S. prison after a plea bargain agreement with a U.S. public prosecutor.[101] He eventually returned to the Netherlands to serve the remainder of his sentence in a

98 In the Netherlands, it is not appropriate to indicate the full name of an individual that has been involved in a criminal investigation. However, Schrooten and a journalist co-authored a book about the events (i.e., David Schrooten and Freke Vuijst, *Alias Fortezza*, Balans 2016) and sought media out to tell the story. In this case, I thus assume it is appropriate to mention Schrooten's full name.

99 See the indictment of *United States v. David Schrooten*. Available at: http://krebsonsecurity.com/wp-content/uploads/2012/06/Schrootenindictment.pdf (last visited on 15 April 2016).

100 See the letter of Defence Counsel Stapert. Available at: http://blogs.vn.nl/download/Brief%20Opstelten-Teeven_3.pdf (last visited on 29 January 2015). See David Schrooten and Freke Vuijst, *Alias Fortezza*, Balans 2016.

101 See Harry Lensink and Freke Vuijst, 'Geen krediet voor David S.', *Vrij Nederland*, 15 April 2013. Available at: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Geen-krediet-voor-David-S.-2.htm (last visited on 3 February 2015).

Dutch prison.[102] The conversion of his sentence to the (much lower) Dutch sentence for the crimes led him to being released soon after his arrival back in the Netherlands.

This case created controversy in the Netherlands, partially due to Schrooten's living conditions in the U.S. prison and the manner in which U.S. law enforcement officials obtained his custody. However, the question also arose as to whether U.S. law enforcement officials had engaged in evidence-gathering activities on Dutch territory and lured Schrooten in order to prosecute him, thereby infringing Dutch sovereignty. In response to parliamentary questions, the Dutch Minister of Security and Justice explained that the Netherlands was aware of U.S. law enforcement authorities' interest in Schrooten, but not of any investigative activities that these authorities were undertaking on Dutch territory.[103] In a 2013 letter to Dutch Parliament the minister stated, similar to the above mentioned letter of 2016 regarding the online pseudo-purchase by DEA agents from an Dutch online drugs dealer, that "no investigative measures have taken place on Dutch territory and no permission was therefore required".[104] This was a remarkable statement, as it was unlikely that U.S. law enforcement authorities were able to obtain necessary evidence against the Dutch suspect and coordinate the extradition by Romanian authorities without conducting any investigative activities on Dutch territory. U.S. law enforcement authorities must have applied the special investigative powers for (1) pseudo-purchase and (2) systematic information gathering on Dutch territory to gather the required evidence. The United States did send the Netherlands a mutual legal assistance request regarding investigation measures in the Netherlands *after* Romania had extradited Schrooten to the United States.[105] It was not specified in the letter which investigative methods the mutual assistance request involved.

---

102 See Harry Lensink, 'Minister wil terugkeer hacker David S. bespoedigen', *Vrij Nederland*, 15 April 2013. Available at: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Minister-wil-terugkeer-hacker-David-S.-bespoedigen.htm (last visited on 29 January 2015).

103 See answers to the parliamentary questions of parliamentary member Van Bommel by the State Secretary of Security and Justice regarding the extradition by Romania of Dutch hacker David S. to the United States on 1 August 2012. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2012/08/01/antwoorden-kamervragen-over-de-uitlevering-van-een-nederlandse-hacker-aan-de-vs-door-roemenie (last visited on 26 October 2015).

104 See answers to parliamentary questions on 12 April 2013, regarding the article 'FBI-agenten hacken mee met Nederlandse politie' and the conditions regarding detention in the United States. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2013/04/16/antwoorden-kamervragen-over-fbi-agenten-hacken-mee-met-nederlandse-politie-en-dententieomstandigheden-vs (last visited on 26 October 2015). See also Harry Lensink and Freke Vuijst, 'Geen krediet voor David S.', Vrij Nederland, 15 April 2013. Available at: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Geen-krediet-voor-David-S.-2.htm (last visited on 3 February 2015).

105 See answers to parliamentary questions of parliamentary member Van Bommel by the State Secretary of Security and Justice on 1 August 2012, regarding the extradition by Romania of Dutch hacker David S. to the United States.

It is possible that U.S. law enforcement officials were not aware of Schrooten's identity and location at the time the undercover investigation took place. His nickname, 'Fortezza', alone did not indicate where he was located. Following their online undercover interactions with the suspect, it can be argued that U.S. law enforcement authorities seized the opportunity to request Romania to extradite him once it became clear that he would land at the airport in that country. It can also be argued that U.S. law enforcement officials already knew the identity of Schrooten and should have requested the Netherlands to prosecute or extradite him. Schrooten himself beliefs that U.S. law enforcement authorities were aware of his location and identity. He claimed that the Secret Service obtained this information based on subscriber information from online service providers and financial transactions that he conducted with the money transmitting service Western Union.[106] It also appears that Russian hackers had previously exposed his identity in online forums, which information may have been gathered by U.S. law enforcement officials.[107]

Regardless of which of these two versions of the extraterritorial evidence-gathering activities in the Netherlands is accurate, the case of David Schrooten illustrates how online undercover investigative methods are used and may lead to questions with regard to both the territorial sovereignty of States and the legal certainty of the individual involved. The case shows how U.S. law enforcement officials factually conducted an online undercover operation that involved a Dutch citizen without requesting prior permission from the Netherlands to conduct the operation or having authorisation derived from a treaty.[108] This means that U.S. laws were applied. As U.S. laws for undercover investigative methods are neither accessible nor foreseeable to Dutch citizens, such a practice endangers the legal certainty of the individuals involved. This case also shows how the cross-border unilateral application of online undercover investigative methods can lead to tension concerning another State's territorial sovereignty.

9.4.2 Dangers to legal certainty

The dangers to the legal certainty of the cross-border unilateral application of online undercover investigative method were illustrated above using the case of David Schrooten. In this case, U.S. regulations for undercover investigative methods were applied that interfered with the rights and freedoms of a Dutch citizen. These regulations were not accessible or foreseeable to

106 See David Schrooten and Freke Vuijst, *Alias Fortezza*, Balans 2016, p. 42.

107 See Brian Krebs, 'Feds Arrest 'Kurupt' Carding Kingpin?', KrebsonSecurity blog, 12 June 2012. Available at: http://krebsonsecurity.com/2012/06/feds-arrest-kurupt-carding-kingpin/ and http://krebsonsecurity.com/wp-content/uploads/2012/06/kuruptru.png (last visited on 15 April 2015).

108 Again, this may be explained by the argument that U.S. law enforcement officials were not aware of Schrooten's identity and location.

Schrooten. In other words, his legal certainty was endangered and an arbitrary interference with his privacy took place. Public sources and case law indicate that U.S. law enforcement authorities extensively use undercover investigative methods in an online context.[109] However, these sources and cases do not indicate that U.S. law enforcement authorities deliberately engage in extraterritorial evidence-gathering activities. It is unclear whether they were aware where the suspect was located. It is only clear that they also apply undercover investigative methods in an online context.

This subsection highlights differences in regulations for undercover investigative methods by briefly comparing the current regulations for undercover investigative methods in the Netherlands and the United States. The Dutch legal framework for undercover investigative methods has already been examined extensively in chapter 7. A summary of the results of that analysis is provided under A below. A brief analysis of the U.S. (federal) regulations for the investigative method is then presented under B. Finally, the most important differences between these regulations are identified under C.

A Overview of Dutch regulations

Certain undercover investigative methods are regulated in detail in Dutch criminal procedural law. Undercover investigative methods are generally viewed as interfering with the right to privacy. Those undercover investigative methods that interfere with the right to privacy in a more than minor manner or threaten the integrity of criminal investigations are regulated as special investigative powers in Dutch law. The number of procedural safeguards that apply depends on how intrusive the investigative power is and the risks they pose to the integrity of investigation.

The analysis in chapter 7 showed that online pseudo-purchases are regulated by the special investigative power for pseudo-purchases in criminal

109 See, e.g., U.S. Department of Justice Office of Public Affairs, 'Alleged International Credit Card Trafficker Arrested in France on U.S. Charges Related to Sale of Stolen Card Data', 11 August 2010. Available at: http://www.fbi.gov/atlanta/press-releases/2010/at081110.htm, Kevin Poulsen, 'The Secret Service Agent Who Collared Cybercrooks by Selling Them Fake IDs', *Wired*, 22 July 2013. Available at: http://www.wired.com/2013/07/open-market/ and Kari Paul, 'An Undercover Agent Was Making $1000 a Week in Bitcoin as a Silk Road Admin', *Motherboard*, 14 January 2015. Available at: http://motherboard.vice.com/read/cirrus-bitcoin-buck. All websites last visited on 30 July 2015. See also, e.g., the FBI press release, 'Child Predators. The Online Threat Continues to Grow', 17 May 2011. Available at: https://www.fbi.gov/news/stories/2011/may/predators_051711 (last visited on 17 July 2015). See also the following extract from the press release: "*During investigations, agents sometimes pose online as teens to infiltrate paedophile networks and to gather evidence by downloading files that are indicative of child pornography. During the investigation of known suspects, undercover agents may also 'friend' people the suspect is associated with*". Case law is referred to in this section under B.1.

procedural law. Authorisation from a public prosecutor is required to apply this special investigative power.[110]

Online undercover interactions with individuals derive from either the general legal basis in art. 3 of the Dutch Police Act or the detailed regulations concerning the special investigative power for systematic information gathering. The analysis in chapter 7 showed that ambiguity exists with regard to when this investigative method is considered to be 'systematically' applied and thus requires the application of the special investigative power. In addition, it was argued that the procedural safeguard for the special investigative power of authorisation from a public prosecutor is not sufficient. Instead, it is preferable that both authorisation from a public prosecutor and supervision by an investigative judge are required, due to the investigative method's intrusiveness vis-à-vis privacy interferences and risks regarding the investigation's integrity, given that entrapment may occur. Dutch law enforcement officials must ensure that a civilian does not commit a crime that he would not have committed without the intervention of law enforcement authorities.

Online infiltration as an investigative method is regulated by the special investigative power for infiltration in the Netherlands. This investigative power is different from systematic information in the sense that it authorises law enforcement officials to participate in a criminal organisation and commit certain crimes when necessary. It was argued that Dutch law should also introduce the mandatory supervision of an investigative judge for the special investigative power for infiltration.[111]

B Overview of U.S. regulations

The U.S. regulations for online undercover investigative methods are first examined with regard to the Fourth Amendment to the U.S. Constitution under B.1. This analysis determines whether a warrant is required to apply undercover investigative methods. As no criminal procedural regulations are applicable to these investigative methods, the most relevant and available internal guidelines for (federal) U.S. law enforcement authorities are examined in B.2 to determine the scope of the methods and the manner in which they are applied.

B.1 Fourth Amendment to the U.S. Constitution

The U.S. Supreme Court has decided in several important cases that the Fourth Amendment does not apply with regard to undercover investigative

110 Although the examined case law in subsection 7.2.1 also revealed that, in practice, an online pseudo-purchase is sometimes applied upon the basis of art. 3 of the Dutch Police Act and authorisation by a public prosecutor is not obtained or too late in the investigation.

111 See chapter 7. Figure 7.1 in the introduction to that chapter visualises the intrusiveness of the investigative method according to Dutch law, with the detail of the law and procedural safeguards that currently apply as regulations for the investigative methods.

methods that are applied by U.S. law enforcement officials.[112] These cases lead to the conclusion that U.S. citizens do not have a reasonable expectation of privacy when they interact with other individuals and must assume that those with whom they are communicating may be law enforcement officials. As such, no warrant is required for undercover operations.

The doctrine that individuals do not have reasonable expectation of privacy when they voluntarily disclose incriminating information to another person is called the '*misplaced trust doctrine*' (cf. Petrashek 2010, p. 1528).[113] The doctrine also applies in an online context. For example, the misplaced trust doctrine permits U.S. law enforcement officials to add themselves as a friend to the Facebook profile of a suspect, or the friends of a suspect, in order to obtain private information about that suspect without a warrant (cf. Semitsu 2011, p. 346 and Petrashek 2010, p. 1528). Several U.S. courts also authorised U.S. law enforcement officials to pose as a minor in chat rooms in order to gather evidence about suspects of online child abuse crimes (see Global Information Sharing Initiative 2013, p. 23).[114]

As stated above, no regulations in U.S. criminal procedural law restrict the application of undercover investigative methods by (federal) law enforcement authorities. Ross (2007, p. 511) explains that undercover investigative methods are instead restricted by (1) internal guidelines of U.S. law enforcement authorities, (2) ethical rules for prosecutors (which forbid undercover contacts with suspects that already have a lawyer), and (3) the prohibition of entrapment.

---

112 See, most notably, U.S. Supreme Court 27 May 1963, *Lopez v. United States*, 373 U.S. at 427 (1963), U.S. Supreme Court 12 December 1966, *Lewis v. United States*, 385 U.S. at 206 (1966) and U.S. Supreme Court 12 December 1966, *Hoffa v. United States*, 385 U.S. at 293 (1966) and U.S. Supreme Court 20 October 1970, *United States v. White*, 401 U.S. at 745 (1971). See Maclin 1996 for a historical analysis of case law with regard to the Fourth Amendment and undercover investigative methods.

113 See also U.S. Supreme Court 12 December 1966, *Hoffa v. United States*, 385 U.S at 302 stating that the Fourth Amendment does not protect *"a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"*.

114 See, e.g., U.S. Superior Court of Pennsylvania 28 march 2001, *Commonwealth v. Proetto*, 771 A.2d 823 (2001) in which U.S. law enforcement officials posed as a 15-year-old girl in a chat room. The suspect made sexually suggestive comments to the "underage female", which the U.S. law enforcement officials logged. The U.S. court reasoned that because the suspect communicated freely with the undercover agent and could not verify the law enforcement's official identity, he had no reasonable expectation of privacy in the chat communications. See also U.S. Court of Appeals for the Armed Forces, 21 November 1996, *United States v. Maxwell*, no. 95-0751 (1996) in which the U.S. court decided the suspect had no reasonable expectation of privacy in e-mail communications with an undercover U.S. law enforcement official, U.S. Court of Appeals of Ohio 6 February 2004, *Ohio v. Turner*, App. 3d 177 (2004), in which the court held that the suspect has no reasonable expectation of privacy in a chat room conversation with an undercover U.S. law enforcement official posing as an underage boy, and U.S. United States Court of Appeals (5th Circuit) 17 February 2010, *U.S. v. Underwood*, no. 08-31243 (2010), in which the U.S. law enforcement officer created an undercover profile purporting to be a 13-year-old boy and sent a friend request to the defendant. The defendant engaged the undercover officer in communication on the MySpace and Yahoo! Web sites, with much of the conversation having a sexual nature.

The prohibition of entrapment was developed in case law that applies to law enforcement officials who use undercover investigative methods. In brief, the U.S. entrapment doctrine dictates that U.S. law enforcement officials are not allowed "to induce an individual to commit an offense, who was otherwise not personally disposed to commit the offense".[115] Kerr explains that the 'inducement of a crime' occurs when an undercover agent pressures a suspect to commit an offence, by either badgering or encouraging him commit the offence in a calculated manner that is based on the suspect's personality (Kerr 2009, p. 591).[116] The suspect's predisposition to committing crimes (called the subjective test) is the most important factor in deciding whether some was pressured into committing a crime.[117] The behaviours of undercover agents are therefore to a (much) lesser extent decisive in determining whether entrapment has taken place (see Joh 2009, p. 172). Joh also observes that: "*the doctrine has not prompted courts to devise a 'meaningful definition of what constitute(s) impermissible participation in the offense' by the police. Most instances of police participation will not constitute entrapment so long as the defendant was a ready and willing criminal.*" In other words, the United States has adopted an entrapment test that differs significantly from the test used in the Netherlands, which also takes the active role of law enforcement officials explicitly into consideration (cf. Kruisbergen & De Jong 2010, p. 116). As a result, undercover law enforcement officials in the United States may, for example, sell illegal goods and then arrest individuals who were predisposed and bought them (Kruisbergen & De Jong 2010, p. 116). This undercover investigative method is not allowed in the Netherlands.[118]

B.2 Guidelines for U.S. law enforcement authorities

In the United States, undercover investigative methods are restricted by internal guidelines for law enforcement authorities. The Guideline for FBI Undercover Operations is briefly examined below, as it provides information with regard to the scope of the investigative methods and the manner in which they are applied in practice.[119]

In the United States, undercover investigative methods are not distinguished and regulated in a similar manner as in the Netherlands. For example, the regulations do not specify when undercover interactions with individuals undertaken by law enforcement officials are applied systematically and thus require special permission (cf. Kruisbergen & De Jong 2010, p. 112).

115 U.S. Supreme Court, *United States v. Russell*, 24 April 1973, 411, at 436 (1972).

116 With reference to U.S. 1st Circuit Court, *United States v. Gendron*, 28 February 1994, 955, at 961-962 (1994).

117 See U.S. Supreme Court, *Sorells v. The United States*, 19 December 1932, 287 U.S. 435 (1932), 356 U.S. Supreme Court, *Sherman v. United States*, 19 May 1958, 356 U.S. 369 (1958) and U.S. Supreme Court *Jacobson v. United States*, 6 April 1992, 503 U.S. 550 (1992).

118 See also explicitly section 2.8 under 'pseudo-selling' in the Guideline for Special Investigative Powers.

119 See the Attorney General's Guidelines on FBI Undercover Operations of 2002.

In the United States, undercover investigative methods are not restricted to particular crimes and do not require approval from a public prosecutor (cf. Ross 2007, p. 562). However, the aforementioned guidelines indicate that permission to conduct an undercover operation must be obtained from a 'Special Agent in Charge' at a local FBI office.[120] The request must detail why the proposed investigation will be effective and that it will be conducted in a minimally intrusive way. The Special Agent in Charge can then authorise undercover FBI agents to participate in certain offences, such as paying bribes, laundering money, and making controlled drug deliveries (so long as these deliveries do not enter the market) (Joh 2009, p. 177). Participation in more serious crimes requires advance approval from FBI headquarters (see Ross 2004, p. 587).[121] Undercover agents are only allowed to commit crimes (1) when necessary to obtain evidence that is not 'otherwise reasonably available', (2) to establish or maintain cover, or (3) to prevent serious bodily injury.[122] The guideline prescribes that "all reasonable steps must be taken to minimize the participation by FBI agents in illegal activity".[123] As explained in subsection 9.2.3, the appendix about 'On-line investigations' by FBI agents is classified. However, other local guidelines also indicate that authorisation is required for U.S. law enforcement officials to interact with individuals on the Internet in an undercover capacity and that 'authorisation levels' are comparable to other undercover investigative-activities in the physical world (cf. Global Information Sharing Initiative 2013, p. 14).[124]

C Notable differences

The Netherlands and the United States have fundamentally different approaches with regard to regulation of undercover investigative methods. In the Netherlands, most undercover investigative methods are regarded as privacy intrusive investigative methods that pose risks with regard to the integrity of criminal investigations. For that reason, certain undercover investigative methods are regulated in specific provisions in criminal procedural law. In the United States, however, undercover investigative methods are not seen as interfering with the privacy of individuals (cf. Kruisbergen et

120 See the Attorney General's Guidelines on FBI Undercover Operations of 2002, p. 4.

121 Joh (2009, p. 177) explains that when sensitive circumstances exist, such as when public officials or media organisations are targeted by an undercover operation, an undercover review committee must approve the operation. That committee consists of officials from the U.S. Department of Justice and the FBI.

122 See Attorney General's Guidelines on FBI Undercover Operations of 2002, p. 12.

123 See Attorney General's Guidelines on FBI Undercover Operations of 2002, p. 12.

124 See specifically the guideline of the U.S. Georgia Bureau of Investigation Investigative Division which states that agents can be authorised using an online alias to interact with a person on social media, when there is reason to believe that criminal offences have been, will be, or are being committed. The example is then provided of *"internet chat rooms where child exploitation occurs"*. The request must mention: (1) which online alias is used, (2) which social media accounts are utilised, (3) the valid law enforcement purpose, and (4) the anticipated duration for the undercover activity (see Global Information Sharing Initiative 2013, p. 32).

al. 2011, p. 398 and Ross 2007, p. 512). Undercover investigative methods are only restricted in internal guidelines, which regulations may vary between local and federal U.S. law enforcement authorities. Individuals involved in U.S. undercover operations cannot derive any rights from these guidelines.

The prohibition of entrapment forbids law enforcement officials in both States from enticing an individual to commit an offence that he did not intend to commit. However, the United States relies more heavily on the subjective test, which means that a suspect's predisposition to committing a crime is particularly important for determining whether entrapment has occurred. In the Netherlands, the active role of law enforcement officials in enticing an individual to commit an offence is also important for determining possible entrapment. As a consequence, U.S. law enforcement officials can play a more active role in undercover operations. For example, U.S. law enforcement authorities have extensive experience in posing as a minor in online chat rooms in child abuse investigations, whereas the legitimacy of this kind of undercover operations is debatable in the Netherlands.

In terms of legal certainty, these results mean that individuals should be aware that very different regulations apply to undercover investigative methods in the Netherlands and the United States. Dutch citizens will find it difficult to understand U.S. regulations for undercover investigative methods given the different notion of the right to privacy, the lack of statutory law for undercover investigative methods, and the different approach to entrapment under U.S. law.

9.4.3 Section conclusion

The analysis in subsection 9.4.1 has shown that cross-border unilateral online undercover investigations can produce extraterritorial effects when the individuals involved in the investigation are on foreign territory. The legal comparison between the Netherlands and the United States has shown that these States have a different view on the interference with territorial sovereignty that occurs when extraterritorial undercover investigations take place on foreign territory. Historically, U.S. law enforcement authorities have been more willing to conduct extraterritorial investigations using undercover investigative methods than their Dutch counterparts. It is too early to tell whether U.S. law enforcement authorities are still engaging in cross-border unilateral undercover operations, but then in an online context. However, the examined case of David Schrooten indicates that U.S. law enforcement officials have conducted evidence-gathering activities on Dutch territory without (prior) approval and have applied U.S. law to a Dutch citizen.

The willingness of U.S. law enforcement authorities to engage in cross-border unilateral undercover investigative activities can perhaps be explained in part by their different perspective on the right to privacy and undercover investigative methods. In the United States, undercover investigative methods are not considered to be privacy infringing and are not sub-

jected to statutory regulations. In contrast, the use of undercover investigative methods is regarded as a privacy intrusive evidence-gathering activity in the Netherlands.[125] From a Dutch perspective, a foreign law enforcement official's application of domestic regulations on a Dutch citizen without permission or an authorising treaty basis is regarded as a violation of Dutch sovereignty.

However, when the identity and location of the individual involved in an online undercover operation cannot be reasonably determined, it may be more acceptable to apply the investigative method unilaterally and across State borders. In this situation, the extraterritorial effects of the investigative method cannot be reasonably determined. When this exception is accepted, the question remains to which extent law enforcement officials must make efforts to identify and determine the location of the individual involved during the online undercover operation.

9.5 Hacking as an investigative method

This section examines the consequences of the cross-border unilateral application of hacking as an investigative method. Section 9.5.1 explores how the Netherlands and the United States each view the desirable restrictions for the cross-border unilateral application of this investigative method. Section 9.5.2 then compares how the two States regulate the method to identify the regulatory differences that illustrate the dangers to legal certainty. Finally, a section conclusion is provided in subsection 9.5.3.

9.5.1 Interferences with territorial sovereignty

The Netherlands and the United States agree that as part of territorial sovereignty, States themselves regulate under which circumstances law enforcement officials can search computers that are located on their territory.[126] When law enforcement officials conduct a search remotely on a computer that is located in another State, the territorial sovereignty of the affected

125 Of course, State power may also be a factor in the sense that other States may be reluctant to engage in extraterritorial evidence-gathering activities on U.S. territory, because the sanctions imposed by the United States for such a practice may have serious consequences for the State involved. It is difficult to estimate whether that is indeed a realistic scenario.

126 With regard to Dutch legislative history, see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (explanatory memorandum Computer Crime Act I), p. 11-12, *Kamerstukken II* (Parliamentary Series Second Chamber) 2004/05, 26 671, no. 10, p. 13. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 48. In the United States, the manual for securing electronic evidence developed by the U.S. Department of Justice warns that: *"in the event that U.S. law enforcement authorities inadvertently access a computer located in another State, appropriate government authorities should be consulted immediately" because "issues such as sovereignty may be implicated"* (DoJ Manual 2009, p. 58).

State may be infringed if no permission has been obtained and no authorising treaty basis is available.[127]

The extraterritorial effects of remotely accessing a computer are localised based on where the data that is stored within a computer system (cf. Koops & Goodwin 2014, p. 61). In order words, a 'computer-orientated jurisdiction principle' is used to localise the effects of hacking as an investigative method. In their extensive analysis regarding the applicable law to 'transborder access to computer systems', i.e., remote access to computers located anywhere without permission of the affected State or the use of legal assistance mechanisms, Koops and Goodwin (2014, p. 61) summarise the current view in international law as follows:

"the most solid view on what international law permits is that accessing data that are, or later turn out to be, stored on a server located in the territory of another state constitutes a breach of the territorial integrity of that state and thus constitutes a wrongful act (...) except where sovereign consent has been formally given".

However, this 'solid view in international law' frustrates law enforcement authorities. When the territorial restriction of enforcement jurisdiction is strictly interpreted and international law is fully respected, law enforcement officials cannot gain access to computer systems on foreign territory. No treaty basis that allows States to gain transborder access to computers is available. The Convention on Cybercrime only allows for this practice in very limited circumstances, namely when the data is publicly available to anyone or permission is obtained from the individual who has rightful access to that information (i.e., the suspect).[128]

The territorial restriction of enforcement jurisdiction in the context of hacking as an investigative method can lead to situation in which law enforcement officials are not able to gather evidence related to an individual who is located in their own State, because an individual uses an online service provider that stores or processes data on foreign territory. For example, Dutch law enforcement officials cannot access an interconnecting computer during a network search when that computer is located on foreign territory.[129] This interpretation severely restricts their possibilities for using network searches to gather evidence from interconnecting computers, since many online services make use of cloud computing and distribute their storage and processing activities among data centres all over the world. Dutch law enforcement officials would then have to assume that the data is likely

127 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (explanatory memorandum Computer Crime Act I), p. 11.

128 See art. 32(a)(b) of the Convention on Cybercrime.

129 See *Kamerstukken II* (Parliamentary Series Second Chamber) 2004/05, 26 671, no. 10, p. 13. An exception applies, for the situation that Dutch law enforcement officials can reasonably assume that the data is located in the Netherlands (*Kamerstukken II* (Parliamentary Series Second Chamber) 2004/05, 26 671, no. 10, p. 23).

stored or processed outside Dutch territory and cannot be obtained (see Koops et al. 2012b, p. 36). This assumption would in turn prevent Dutch law enforcement officials from using a network search to gain access to online services, such as webmail and online storage services.[130]

In my view, the following question should be addressed: Is the territorial sovereignty of the United States violated if Dutch law enforcement officials can access data related to a Dutch citizen who utilises a U.S. online service provider? That data is not necessarily located in the United States. In my view, cross-border unilateral network searches and remote searches should be possible when the following three requirements are met: (1) the individual who is involved in the criminal investigation is located in the investigating State, (2) law enforcement officials already possess the login credentials necessary to access the servers (hosting the content in the online account), and (3) a warrant to perform the search has been obtained from an investigative judge (Conings & Oerlemans 2013, p. 29-30).[131] In this situation, the interference with territorial sovereignty that occurs is not severe, since it is unclear where the interference takes place and which State is affected (cf. Koops & Goodwin 2014, p. 76 and Conings 2014, p. 14). In addition, the legal certainty of the individual involved is not endangered, because the cross-border unilateral access is conducted from a computer on the territory of the investigating State (where that individual is located).

In addition, when criminals utilise a system such as Tor, the network they use to access the Internet is obscured. Are law enforcement authorities then no longer allowed to remotely access a computer system under their own jurisdiction, because the computer that is accessed *might* be located on foreign territory? Similarly, when a criminal utilises anonymising services, such as proxy services and VPN services, it may not be possible to identify the computer user.[132] The use of anonymising services and cloud computing services have prompted the Dutch legislature and U.S. law enforcement authorities to propose an exception to the territorial limitation of enforcement jurisdiction, in order to allow for the cross-border unilateral application of hacking as an investigative method in special circumstances. These proposals are briefly examined below.

A The Dutch proposal

In its explanatory memorandum attached to the Computer Crime Act III, the Dutch legislature took a bold position with regard to the cross-border unilateral application of hacking as an investigative method. That memoran-

130 See the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53. See also subsection 8.2.1.

131 For instance, law enforcement officials can obtain these login credentials from a seized computer. They can then be used to gain access to the online account(s) of a suspect.

132 For instance, because the proxy service provider or VPN provider is located in a State that does not cooperate with law enforcement authorities of the investigating State, or because these providers did not log subscriber data and traffic data that is necessary to identify internet users.

dum states that "*when the location of the data cannot be reasonably determined*", remote access to that data is authorised.[133] As explained in the memorandum, this situation arises when suspects utilise services that enable cloud computing or anonymising services or techniques.[134] When the location of the data that is stored on computers is known, then permission of the State that will be affected by the investigative method is required or mutual legal assistance must be requested.[135] The main reason for this position is that the Dutch legislature wants to prevent the Internet from becoming a 'free haven' for criminals, which leads it to viewing certain forms of unilateral action as simply necessary (and apparently acceptable).[136]

The Computer Crime Act III proposes a new special investigative power that would enable Dutch law enforcement officials to remotely access a computer and then conduct a remote search and use policeware.[137] The proposal specifies that these officials would need to take the following factors into consideration when determining whether cross-border unilateral action is allowed:

(1) the seriousness of the crime;
(2) the degree of the involvement of the Netherlands (either by Dutch victims or the use IT infrastructure located in the Netherlands);
(3) the nature of the investigative techniques (e.g., remotely disabling data is deemed more intrusive than remote copying); and
(4) the risks for the integrity of the computers involved.[138]

These factors can indeed aid in interpreting the proportionality and subsidiary test that Dutch law requires be used when special investigative powers are applied. In my view, what is clearly missing from the explanatory memorandum is an understanding of the sensitivity and possible political repercussions of investigative activities that take place on foreign territory. Hacking as an investigative method is very intrusive investigative method. It is more likely that States will object when this investigative method is applied to a computer located on their territory than when other investigative methods are used, such as an online undercover investigation that only involves interaction with other individuals. In addition, unilateral hacking as an investigative method will make other States feel entitled to take recip-

133 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 51.
134 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 52.
135 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 46-47.
136 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 51
137 See also section 2.4 of chapter 8. The proposal also includes other types of hacking as an investigative method, but these are not examined in this study.
138 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 52

rocal actions in the form of using hacking as an investigative method from their own territory (cf. Koops & Goodwin 2014, p. 77 and AIV report 2014, p. 61). This aspect should also be explicitly taken into consideration when a decision is made to (allow for) remote access to a computer to gather evidence.

B The U.S. proposal

In the United States, U.S. criminal procedural law regulates the conditions under which a search warrant can be obtained to search a computer. In particular, Rule 41 of the U.S. Federal Rules of Criminal Procedure dictates the conditions for obtaining warrants to conduct searches, including remote searches. In brief, a 'Rule 41 search warrant' mirrors the requirements of the Fourth Amendment but adds extra requirements. The relevant rule dictates that a magistrate judge can issue a warrant at the request of a federal law enforcement officer or an attorney to search a place and 'seize particularly described things' (including digital information) in order to find evidence or contraband, when probable cause exists that the evidence or contraband is to be found at that place. The warrant can authorise governmental officials to seize 'electronic storage media' or 'seize or copy electronically stored information' in computers.

The text of Rule 41 currently restricts the warrant to "*the district of the court of the magistrate judge*". This restriction significantly limits the possibilities to conduct a remote search or install policeware in computers, since these investigative methods can only be applied within the district of the court of the judge.[139] The U.S. Department of Justice therefore seeks to amend Rule 41 to enable 'remote access' to computers and thus facilitate hacking as an investigative method. Its proposal is to amend Rule 41 so that its text holds that *"a magistrate judge with authority in any district where activities related to a crime may have occurred, has the authority to issue a warrant to use remote access to search electronic storage and to seize or copy electronically stored information located within or outside that district"*.[140]

With this proposal, the U.S. Department of Justice seeks to make remote searches possible in the following three situations: (1) when the district where the media or information is located has been concealed through technological means (e.g., by using anonymising software such as Tor), (2) when the victimised computers are located in five or more U.S. judicial districts (which typically applies when botnets are involved in cybercrimes), and (3) in the search of information that is accessible from a computer but is stored remotely in another district (e.g., remotely accessible cloud-based services

139 See Rule 41(b)(1): *"a magistrate judge with authority in the district-or if none is reasonably available, a judge of a state court of record in the district-has authority to issue a warrant to search for and seize a person or property located within the district"*.

140 The proposed amendment is available at: http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Standing/ST2014-05.pdf (last visited on 30 December 2014). See p. 499 and 500 and p. 600. Emphasis added by the author.

or web-based e-mail of an individual) (cf. Schwerha IV 2015, p. 2-3).[141] The U.S. Supreme Court used a special procedure to accept these changes in April 2016. The proposal was subsequently forwarded to the U.S. Congress, which now has until 1 December 2016 to halt or accept the amendment.[142]

Comparison of the proposals

The Dutch legislature and the U.S. Department of Justice have thus both proposed to allow hacking as an investigative method in similar situations. Simply stated, cross-border unilateral hacking as an investigative method is deemed permissible when the individuals involved in the criminal investigation utilise services that enable cloud computing or utilise anonymising services or techniques.

These approaches can be regarded as an exception to the generally accepted interpretation of the territorial restriction of enforcement jurisdiction that States cannot access computers on foreign territory without permission from the affected State or a treaty basis. Goldsmith (2001, p. 117-118) submits that certain applications of hacking as an investigative method with extraterritorial effects may even become customary among States.[143] I expect that law enforcement authorities all over the world will increasingly use hacking as an investigative method. As illustrated in this subsection, States can deem the cross-border unilateral application of hacking as an investigative method as necessary to overcome the obstacles of anonymity, encryption, and jurisdiction in cybercrime investigations. However, it is also conceivable that certain law enforcement authorities will apply the investigative method simply because it is a convenient way to gather evidence. The conditions under which cross-border unilateral hacking as an investigative method is ultimately accepted among States will depend on domestic legislation in individual States and responses within the international community.

141 See also p. 499 and 500 of the proposed amendment to Rule 41.

142 See, e.g., Danny Yadron, 'Supreme court grants FBI massive expansion of powers to hack computers', *The Guardian*, 29 April 2016. Available at: https://www.theguardian.com/technology/2016/apr/29/fbi-hacking-computers-warrants-supreme-court-congress (last visited on 25 May 2016).

143 Goldsmith argued that cross-border unilateral remote searches should not be regarded as an infringement of another State's sovereignty, but instead as part of *"the inevitably messy process of working out new customary principles of sovereignty to accommodate a new and important, but also potentially dangerous, technology"* (Goldsmith 2001, p. 117-118). Of course, at the same time, it should be pointed that States can only object to a practice when States are aware of the application of hacking as an investigative method and States claim responsibility for it.

9.5.2 Dangers to legal certainty

Hacking as investigative method is a particularly intrusive investigative method that seriously interferes in the rights and freedoms of the individuals involved. When foreign law enforcement officials gain remote access to a computer of a citizen on foreign territory, that individual's legal certainty is endangered.

This subsection highlights the differences in the regulations for hacking as an investigative method using a brief comparison of the Dutch and U.S. situations. The Dutch legal framework for hacking as an investigative method has already been examined extensively in chapter 8. A summary of the results of that analysis is provided under A below. A brief analysis of the U.S. (federal) regulations for the investigative method is then conducted under B. Finally, the most important differences between Dutch and U.S. regulations are identified under C.

A Overview of Dutch regulations

Hacking as investigative method has been categorised as (1) network searches, (2) remote searches, and (3) the use of policeware. The analysis in chapter 8 has shown that in the last five years, the regulations and procedural safeguards that apply to regular powers for searching a place and seizing computers have been used as a legal basis for network searches and remote searches. Remote searches are considered as more privacy intrusive than network searches, since they can be applied covertly (whereas network searches must still be conducted during a search at a particular place). The use of policeware can be derived from the existing legal basis for recording private communications, which is also regulated as a special investigative power in Dutch law. However, in order to use all functionalities of policeware, i.e., those that go beyond the recording of private communications (such as taking screen shots), special provisions with appropriate procedural safeguards must be created. Using policeware is considered to be the most privacy intrusive investigative method examined in this study, given that it involves remote access to computer systems, is applied covertly, and enables law enforcement officials to both take specific functions of computers over and monitor an individual's computer behaviours.

The Dutch legislature now has to decide whether to accept the proposal for a new Computer Crime Act (i.e., Computer Crime Act III), which includes the special investigative power to 'gain remote access to computers' (i.e., to hack computers). The proposed special investigative power incorporates remote searches and the use of policeware, but excludes network searches that are already regulated in a separate investigative power in the DCCP. The proposal for a special investigative power for hacking as an investigative method details appropriate strong procedural safeguards.[144]

144 In chapter 8, concerns were raised with regard to the scope of the proposed special investigative power.

However, it was argued Dutch legislature should scrutinise the scope of the proposed special investigative power. It was also argued that the special investigative power for network searches should include a warrant requirement from an investigative judge.

B Overview of U.S. regulations for the investigative method

The U.S. regulations for hacking as an investigative method are first examined with regard to the method's relation to the Fourth Amendment to the U.S. Constitution. This analysis determines whether a warrant is required to apply this investigative method. The regulations in U.S. criminal procedural law (namely Rule 41 of the U.S. Federal Rules of Criminal Procedure) were already examined in subsection 9.5.1 and are not repeated here.[145]

Fourth Amendment to the U.S. Constitution

When U.S. law enforcement officials undertake domestic investigations, they most often have to obtain a warrant to apply hacking as investigative method as meant in this study. The distinguished types of hacking as an investigative method, i.e., (1) network searches, (2) remote searches, and (3) the use of policeware, can all be applied insofar as a warrant is obtained from a U.S. judge. More particularly, U.S. law enforcement officials typically need to acquire a Rule 41 warrant, as described in subsection 9.5.1.

A warrant is required because gaining remote access to a computer (the first step when performing hacking as an investigative method) can essentially be regarded as a 'search' when considered in the context of the Fourth Amendment to the U.S. Constitution. In the United States, computers are viewed as 'containers', analogous to letters, packages, boxes, and trunks (cf. Kerr 2010, p. 309). In this regard, the basic rule is that individuals have a reasonable expectation of privacy with regard to a container's contents. As a result, the Fourth Amendment warrant requirement generally applies to the seizure of computers and subsequent search and seizure of the data within them (cf. Kerr 2010, p. 309).[146]

However, whether the Fourth Amendment also protects the seizure of computers and subsequent search and seizure of their data that takes place directly after an arrest was debated until 2014.[147] This so-called 'search incident to arrest' exception to the warrant requirement enabled law enforcement officials to seize a computer within a reasonable time following an arrest without having to obtain a warrant from a U.S. judge.

---

145 The manual for Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations of the U.S. Department of Justice (DoJ Manual 2009) is also referred to when it provides additional relevant information. The manual does not refer to the use of remote searches or policeware as investigative methods. However, it does indicate that a warrant is required for a network search (see DoJ Manual 2009, p. 84).

146 In the United States, exceptions for searching computers at national borders (e.g., at airports) apply. These exceptions are not further examined in this study.

147 See, e.g., Brenner 2011 and Gershowitz 2008.

In the landmark 2014 case of *California v. Riley*, the U.S. Supreme Court decided that a warrant is required to seize a cell phone immediately following an arrest.[148] Due to this decision, the 'search incident to arrest' exception no longer applies in the United States. The U.S. Supreme Court asserted that today's cell phones should not be treated as regular objects. This view is reflected in the *Riley* decision as follows:

"Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life," (...). The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant."[149]

The facts that cell phones are no longer regarded as regular objects and law enforcement offices must obtain warrants to seize and subsequently search and seize their contents also leads to the conclusion that the warrant requirement also applies to other computers. A (Rule 41) warrant is therefore also required to perform a network search (cf. DoJ Manual 2009, p. 84-85) or remote search (cf. Brenner 2012).

From case law, it is also clear that U.S. law enforcement officials must obtain a Rule 41 warrant to utilise policeware.[150] In a 2013 judgement, a U.S. judge denied a warrant request for using policeware. The request stipulated that that warrant was needed to enable federal law enforcement officials to:

"surreptitiously install data extraction software on the Target Computer. Once installed, the software has the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within the district."[151]

The case thus confirms that U.S. law enforcement authorities require a (Rule 41) warrant to use policeware. The description of the functionalities of the policeware also indicate the scope of the investigative method.

148 U.S. Supreme Court, 25 June 2014, *Riley v. California*, 573 U.S. (2014).

149 U.S. Supreme Court, 25 June 2014, *Riley v. California*, 573 U.S., at 32 (2014).

150 However, data access requests have revealed that U.S. law enforcement officials remotely installed and used policeware as early as 2007. See Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', *Wired*, 18 July 2007. Available at: http://archive.wired.com/politics/law/news/2007/07/fbi_spyware (last visited on 30 December 2014).

151 See Cyrus Farivar, 'FBI denied permission to spy on hacker through his webcam', *Ars Technica,* 25 April 2013. Available at: http://arstechnica.com/tech-policy/2013/04/fbi-denied-permission-to-spy-on-hacker-through-his-webcam/ (last visited on 30 December 2014).

The U.S. judge denied the warrant request in the above case, on the basis that the Rule 41 requirements (including the territorial limitation of the warrant) were not satisfied.[152] With regard to the dangers to legal certainty, the following statement of the judge is relevant:

"*That search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name*".[153]

This statement eloquently indicates how individuals can be subjected to U.S. governmental power when a warrant is issued to install policeware on a computer with an unknown location. As foreign laws cannot be accessible or foreseeable to individuals, those individuals involved are subjected to arbitrary governmental interference in their private lives.

In summary, U.S. law enforcement authorities in principle require a (Rule 41) warrant to (1) perform a network search, (2) perform a remote search, or (3) make use of policeware. However, an important exception has been formulated in relation to 'computer searches on foreign territory'. This exception is further examined below.

No warrant required for computers outside U.S. territory?

In the landmark case of *United States v. Verdugo-Urquidez*, the doctrine was established that only U.S. citizens and individuals located on U.S. territory are protected by the U.S. Constitution.[154] Following the decision, U.S. law enforcement officials do not require a warrant to search a place of a non-U.S. individual outside U.S. territory. The case is briefly examined below.

The case of *United States v. Verdugo-Urquidez* involved a criminal investigation with regard to drug trafficking and the murder of a U.S DEA agent. In this case, U.S. DEA law enforcement officials worked together with local Mexican authorities. The U.S. law enforcement authorities searched a residence located on Mexican territory without a U.S. warrant. However, the local Mexican law enforcement authorities reportedly authorised the U.S. law enforcement officials to perform the search. The U.S. law enforcement officials found records of marijuana shipments made by the suspect inside the residence, who was subsequently brought to the United States for trial. When the suspect protested that U.S. law enforcement authorities were supposed to obtain a warrant to search his residence in Mexico, the U.S

152 See subsection 9.5.1.

153 See U.S. District Court Southern District of Texas Houston Division, *In Re Warrant To Search a Target Computer at Premises Unknown*, 22 April 2013, 958 F.Supp.2d 753.

154 U.S. Supreme Court 28 February 1990, *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

Supreme Court decided that U.S. law enforcement officials do not require a warrant to search the residence of a non-U.S. citizen on foreign territory.[155]

As a result of the *United States v. Verdugo-Urquidez* case, U.S. law enforcement officials who undertake search and seizures measures as outside U.S. territory in situations that do not involve a U.S. citizen do not require a warrant under the Fourth Amendment to the U.S. Constitution (cf. Gane & Mackarel 1996, p. 109, Vander Beken 1999, p. 249). Milanovic (2015, p. 89) describes the doctrine as a manifestation of the idea of a social contract, namely that privacy protections are only awarded to citizens or individuals living on the territory of the investigating State. This doctrine may have consequences for the warrant requirement for using hacking as an investigative method. Two hacking cases that have referred to this doctrine are briefly examined below.

In the case of *United States v. Gorshkov*, FBI officials lured two Russian suspects to the United States for job interviews at the fake IT security company 'Invita' in 2001.[156] During their interviews, the individuals were requested to demonstrate their computer skills by hacking into a network that had been set up by the FBI. The suspects consequently downloaded hacking tools from the website 'tech.net.ru', which was located on their own servers in Russia. The FBI agents had installed a keylogger on the laptop they provided to the Russian suspects, which enabled them to subsequently record the login credentials that the suspects used to gain access to two servers located on Russian territory. The U.S. Department of Justice reportedly requested legal assistance from Russian authorities to obtain the data from the Russian servers, but they did not receive a reply. After several unsuccessful attempts to convince the Russian authorities to co-operate, the FBI used the collected usernames and passwords to access the two servers and subsequently download a total of 1.3 gigabytes of information from them.[157] During the trial, it became apparent that the FBI agents had downloaded the files from the Russian server without a warrant (which was obtained later in

155 U.S. Supreme Court 28 February 1990, *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). However, see also Judge Brennan's dissenting opinion at 283-284, stating that: *"What the majority ignores, however, is the most obvious connection between Verdugo-Urquidez and the United States: he was investigated and is being prosecuted for violations of United States law and may well spend the rest of his life in a United States prison. The 'sufficient connection' is supplied not by Verdugo-Urquidez, but by the Government. Respondent is entitled to the protections of the Fourth Amendment because our Government, by investigating him and attempting to hold him accountable under United States criminal laws, has treated him as a member of our community for purposes of enforcing our laws. He has become, quite literally, one of the governed."*

156 See U.S. District Court of Washington, *United States v. Gorshkov*, 23 May 2001, F.Supp.2d, 2001 WL 1024026, 23 May 2001, at 1.

157 Robert Lemos, 'FBI "hack" raises global security concerns', *CNET News*, 1 May 2001. Available at: http://news.cnet.com/FBI-hack-raises-global-security-concerns/2100-1001_3-256811.html (last visited on 30 July 2015).

time) and used the collected data as trial evidence.[158] In response, the Russian Federal Security Service charged one of the involved FBI agents with computer hacking on Russian territory in 2002.[159]

At trial, the Russian suspects objected to the evidence-gathering activity, arguing that they were protected by the Fourth Amendment to the U.S. Constitution, which requires law enforcement officials to have a warrant to conduct a search. With regard to whether a warrant was required, the judge decided that:

"The Fourth Amendment does not apply to the agents' extraterritorial access to computers in Russia and their copying of data contained thereon. First, the Russian computers are not protected by the Fourth Amendment because they are property of a non-resident and located outside the territory of the United States. Under United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), the Fourth Amendment does not apply to a search or seizure of a non-resident alien's property outside the territory of the United States. In this case, the computers accessed by the agents were located in Russia, as was the data contained on those computers that the agents copied. Until the copied data was transmitted to the United States, it was outside the territory of this country and not subject to the protections of the Fourth Amendment"[160]

The judge thus decided that suspects were therefore not protected by the Fourth Amendment. The judge also found that Russian law did not apply either.[161] Their legal position can thus be described as a 'legal vacuum'.

In the case of *United States v. Ross Ulbricht*, a U.S. prosecutor also argued that a warrant is not required to search a computer that is located on foreign territory and belongs to a foreign company (e.g., a hosting provider).[162] The prosecutor's argument was as follows:

158 The data reportedly provided a 'wealth of evidence'. The databases contained more than 56,000 credit cards, bank account information, and other personal information of individuals. See U.S. Department of Justice Press Release, 'Russian Computer Hacker Convicted by Jury', 10 October 2002. Available at: http://www.justice.gov/criminal/cybercrime/press-releases/2001/gorshkovconvict.htm (last visited on 30 July 2015).

159 John Leyden, 'Russians accuse FBI agent of hacking', *The Register*, 16 August 2002. Available at: http://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/ (last visited on 30 July 2015).

160 U.S. District Court of Washington, *United States v. Gorshkov*, 23 May 2001, F.Supp.2d, 2001 WL 1024026, 23 May 2001, at 3. Emphasis added.

161 U.S. District Court of Washington, *United States v. Gorshkov*, 23 May 2001, F.Supp.2d, 2001 WL 1024026, 23 May 2001, at 4: "*As to Defendant's contention that the FBI's actions were unreasonable and illegal because they failed to comply with Russian law, the Court finds that Russian law does not apply to the agents' actions in this case and even if it were to apply, the agents sufficiently complied with the relevant portions of the Criminal Process Code of Russia.*"

162 See subsection 2.3.3 for a more extensive analysis of the Silk Road investigation.

Because the [Silk Road] server was located outside the United States, the Fourth Amendment would not have required a warrant to search the server, whether for its IP address or otherwise (…). Given that the SR server was hosting a blatantly criminal website, it would have been reasonable for the FBI to "hack" in to it in order to search it, as any such "hack" would simply have constituted a search of foreign property known to contain criminal evidence, for which a warrant is not necessary".[163]

The U.S. law enforcement officials never confirmed that they obtained remote access to the server of the Silk Road forum.[164] The contents of the server were eventually acquired using a mutual legal assistance request from law enforcement authorities in Iceland.

However, Brenner and Kerr argue that a warrant is still required when U.S. law enforcement officials remotely access computers on foreign territory, because that investigating activity *also* takes place on U.S. territory as part of a domestic criminal investigation.[165] Indeed, a key characteristic of cross-border unilateral digital investigative activities is that they occur on territory of both the investigating State and another State simultaneously (cf. Forcese 2011). To deny the safeguards that criminal procedural law offers based solely on the fact that the individuals involved are on foreign territory makes no sense (cf. Van der Wilt 2000, p. 186).[166] When neither local nor foreign laws are applied, these individuals are placed in a legal vacuum and deprived of protection from either legal system. It appears that the proposed amendment to the Rule 41 warrant will always require a warrant for U.S. law enforcement officials who want to use hacking as an investigative method.

---

163 See the government response to the declaration of Joshua Horowitz in *United States v. Ross Ulbricht*, S1 14 Cr. 68 (KBF), p. 7. With regard to the facts of the *Silk Road* investigation, see, e.g. Nate Anderson and Cyrus Farivar, 'How the feds took down the Dread Pirate Roberts', *Ars Technica,* 3 October 2013. Available at: http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/, Kim Zetter, 'How the Feds Took Down the Silk Road Drug Wonderland', 18 November 2015. Available at: http://www.wired.com/2013/11/silk-road/, and Joshuah Bearman, 'Silk Road: The Untold Story', *Wired*, 23 May 2015. Available at: http://www.wired.com/2015/05/silk-road-untold-story/ (last visited on 30 September 2015).

164 See Andy Greenberg, 'Ross Ulbricht Calls For New Trial, Alleging Feds Hacked Tor', *Wired*, 9 March 2015. Available at: http://www.wired.com/2015/03/ross-ulbricht-calls-new-trial-alleging-feds-hacked-tor/ (last visited on 30 September 2015).

165 See S. Brenner, 'Our Fourth Amendment', 11 March 2006. Available at: http://cyb3r-crim3.blogspot.nl/2006/03/our-fourth-amendment.html and Orin Kerr, 'Fascinating New Case on Legal Standards for Searching a Remote Computer With Unknown Location', The Volokh Conspiracy (blog), 26 April 2013. Available at: http://volokh.com/2013/04/26/fascinating-new-case-on-legal-standards-for-searching-a-remote-computer-with-unknown-location/ (last visited on 25 January 2015).

166 See also the more articulate dissenting opinion of Judge Brennan in *Verdugo-Urquidez v. United States*, at 283-284: *"Fundamental fairness and the ideal underlying our Bill of Rights compel the conclusion that when we impose societal obligations such as the obligation to comply with our criminal laws, on foreign nationals, we in turn are obliged to respect certain correlative rights, among them the Fourth Amendment."*

C Notable differences

The Netherlands and the United States have different legal frameworks for hacking as an investigative method.

In the Netherlands, the legislature aims to create a new special investigative power for remote searches and the use of policeware in Dutch criminal procedural law. The proposal specifies that law enforcement officials require a warrant from an investigative judge to apply the investigative power. However, the legal basis for network searches is not amended and still mirrors the regulations for computer searches. In the Netherlands, no warrant is required for computer searches, unless the search and subsequent seizure of a computer takes place within a residence.

In the United States, a warrant is required for the identified types of hacking as an investigative method, insofar as a computer is located on U.S. territory or the computer belongs to a U.S. individual. Based on the *United States v. Verdugo-Urquidez* case, it can be argued that the Fourth Amendment only applies to U.S. citizens or computers on the territory of the United States. Kerr and Brenner have argued that the Rule 41 warrant is nevertheless applicable, since the investigation takes place on U.S. territory as well as on foreign territory. Which interpretation U.S. law enforcement authorities have adopted remains unclear.

From a Dutch perspective, the territorial limitation of the Fourth Amendment warrant requirement is peculiar. In the Netherlands, Dutch law also applies when evidence-gathering activities are applied on the territory of another State. In the context of the cross-border unilateral application of hacking as an investigative method, the U.S. territorial limitation of the Fourth Amendment is troubling from the perspective of legal certainty. It is possible that when this investigative method is applied unilaterally across State borders, neither U.S. law nor the domestic regulations of the State where that computer is located are applicable – which puts the citizen involved in a legal vacuum.

9.5.3 Section conclusion

Hacking is an intrusive investigative method that infringes on the territorial sovereignty of another State when the targeted computer is located on foreign territory. For that reason, law enforcement authorities are not allowed to gain remote access to computers that are located on foreign territory without permission from the affected State or a treaty basis that authorises the evidence-gathering activity.

However, the legislative bodies in both the Netherlands and the United States aim to allow cross-border unilateral hacking as an investigative method when, simply put, the location of the computer targeted for remote access is unclear, the search is proportionate considering the circumstances at hand, and no other alternatives for gathering the information are available. Law enforcement authorities in both countries clearly feel the need to deploy hacking techniques to combat cybercrime more effectively (cf. Brenner 2012, p. 91-92).

However, applying cross-border unilateral hacking as an investigative method will make other States feel entitled to take reciprocal actions in the form of applying this investigative method from their own territory (cf. Koops & Goodwin 2014, p. 77 and AIV report 2014, p. 61). It is difficult to foresee the reciprocal effects and thereby the consequences for citizens and companies that may arise were foreign law enforcement authorities to do so. The worst-case scenario would be a situation in which law enforcement authorities hack computers on the territory of other States under their own domestic regulations. In such a 'digital legal jungle' where many local regulations for investigative methods are applied extraterritorially by law enforcement authorities, a State's citizens would not know if law enforcement authorities have obtained (unauthorised) access to their computers and then conducted other investigative activities. They would also not be aware of the conditions for applying hacking as an investigative method in criminal investigations.

9.6 Restrictions for the identified investigative methods

This section examines the desirable restrictions for the cross-border unilateral application of the identified investigative methods. The proposals made are based on the analyses in the previous sections and focus on the evidence-gathering activities that are conducted by Dutch law enforcement officials. These proposals can be considered as a first step towards developing a policy for cross-border unilateral cybercrime investigations. The details of both the desirable procedures and the treaty provisions must be further examined and developed. It is important that all States start to include the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. They should also make an effort to reach agreements with other States as to the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable. The EU should also incorporate the concept of (cross-border unilateral) digital evidence-gathering activities within the EU legal framework for legal assistance. Finally, the Council of Europe should continue its efforts to include States in the Convention on Cybercrime and further develop regulations for 'cross-border access to computers'.

This section further focuses on the desirable restrictions of the cross-border unilateral application of the identified digital investigative methods for Dutch law enforcement authorities. The extent to which it is desirable to apply each identified investigative method unilaterally across State borders is examined separately in subsections 9.6.1 to 9.6.4.

9.6.1 Gathering publicly available online information

The analysis in section 9.2 has shown that gathering publicly available online information that is located on foreign territory likely does not infringe

the territorial sovereignty of other States. The reasons are that States tacitly allow for the cross-border unilateral gathering of this information and the potential infringement to the territorial sovereignty of States appears to be minor. Dutch law enforcement authorities are therefore allowed to gather publicly available online information both across State borders and unilaterally.

However, this practice may endanger the legal certainty of the individuals involved. For example, in the Netherlands, detailed regulations apply in relation to systematic observation of the online behaviours of individuals. When foreign law enforcement officials are allowed to systematically observe the behaviours of Dutch citizens, the domestic regulations for those foreign law enforcement authorities are not foreseeable to the individuals involved. It would be preferable from a fundamental rights perspective if the Netherlands could specify in treaties the conditions under which the systematic online observation of individuals is allowed. However, the extraterritorial gathering of publicly available online information, that typically includes information that can be obtained by observation, is already arguably international customary law. It is also problematic for States to detect the application of the investigative method, due to the nature of the Internet, which practically allow foreign law enforcement authorities to apply the investigative method anonymously, across borders, and in a unilateral manner. I am not convinced that States would be willing to conclude treaty agreements with regard to this evidence-gathering activity, given that their law enforcement officials are already applying it with little chance of repercussions for their actions.

9.6.2 Data production orders

The analysis in section 9.3 has shown that the cross-border unilateral issuance of data production orders to (foreign) online service providers may interfere with the territorial sovereignty of the State where the company is located and the States where the data is stored on computers. As part of their territorial sovereignty, States can decide under which circumstances companies can disclose data to foreign law enforcement authorities.

However, online service providers can provide their services to individuals located anywhere in the world. Online service providers make use of cloud computing, which make it difficult to pinpoint the location of the data and thereby difficult to determine where the extraterritorial effects of the investigative method takes place. A practice has arisen where certain (U.S.) online service providers voluntarily disclose non-content data to foreign law enforcement authorities when (in their eyes) valid data production orders are issued. To obtain content data, it appears that a U.S. warrant and mutual legal assistance is required. The practice of voluntarily disclosure is less burdensome than applying legal assistance mechanisms for law enforcement authorities. However, the voluntarily disclosure of information does endanger the legal certainty of the individuals involved.

Therefore, it is preferable that States negotiate a treaty that regulates unilateral data production orders that are issued to online service providers (cf. De Schepper & Verbruggen 2013, p. 166 and Verbruggen 2014, p. 140). Such a treaty should differentiate between different safeguards to obtain the identified categories of data from online service providers according to their sensitivity and thereby protect the individuals involved. It would be preferable for the Council of Europe to negotiate a provision in the Convention on Cybercrime or an extra protocol, seeing as many States have already ratified the Convention on Cybercrime.

In the past five years, working groups designated by the Council of Europe have been unable to propose amendments or a new protocol to the Convention on Cybercrime to regulate unilateral data production orders (cf. Koops & Goodwin 2014, p. 58). The urgency for regulation will only increase in the future, since the information available at online service providers that is relevant for law enforcement authorities will continue to grow. Alternatively, the EU could attempt to conclude a treaty with the United States that dictates the conditions under which law enforcement authorities can use data production orders to obtain the data of these providers' customers.[167]

9.6.3 Online undercover investigative methods

The analysis in section 9.4 has shown that undercover operations conducted by investigative officials during the course of criminal investigations produce extraterritorial effects that, without consent from or a treaty basis with the affected State, intrude on the territorial sovereignty of that State. For that reason, Dutch law enforcement officials are in theory not allowed to conduct undercover operations that involve individuals who are located on foreign territory (cf. Siemerink 2000a, p. 80). The analysis has also shown that States regulate (online) undercover investigative methods in different ways. In order to respect State sovereignty and the rights and freedoms of the individuals involved, it is recommended that Dutch law enforcement officials seek legal assistance or otherwise obtain permission when they know that an individual involved in an online undercover investigation is on foreign territory. The involvement of foreign law enforcement authorities is often required eventually anyway, given that further criminal procedural powers (such as for searching and seizing physical places and making arrests) will have to be applied by the local law enforcement authorities to successfully prosecute individuals who are located on foreign territory.

---

167 In this respect, the press release of the Council of the European Union on 9 June 2016, 'Fight against criminal activities in cyberspace: Council agrees on practical measures and next steps', in which the council concludes that action is required *"in the area of improving cooperation with service providers, through the development of a common framework (e.g. use of aligned forms and tools) with them to request specific categories of data"*. Available at: http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/ (last visited on 8 June 2016).

However, when the location of the individual involved is unknown, Dutch law enforcement officials should be able to apply cross-border unilateral online undercover investigations. The reason is that the extraterritorial effects of the investigative method cannot be reasonably determined and the legal regime in international law cannot be applied in such a situation. When an individual's location becomes apparent, the investigating law enforcement authorities should notify the relevant State and either obtain permission to continue the operations or initiate mutual legal procedures.

It would be preferable for States to agree on the above-mentioned procedure for online undercover investigative methods in new or existing mutual legal assistance treaties. However, similar to when systematic online observation is applied as an investigative method, it is questionable whether States would be willing to agree on the terms under which undercover systematic interactions with foreign individuals are allowed. It may be difficult for the affected State to detect – and object to – the practice of this undercover investigative method, given the method's limited intrusiveness in terms of intruding on sovereignty. At the same time, the case of David Schrooten illustrates how such an operation can ultimately lead to controversy and unrest in the affected State. States must also consider the reciprocal effects of the online undercover practices of their law enforcement authorities.

9.6.4 Hacking as an investigative method

The analysis in section 9.5 has shown that performing hacking as an investigative method on computers located on foreign territory interferes with the territorial sovereignty of the State where the targeted computer is located. Without permission from that State or an authorising basis in a treaty, the cross-border unilateral application of this investigative method is thus not allowed.

Legislative bodies in both the Netherlands and the United States aim to make the application of cross-border unilateral hacking as an investigative method possible when the location of the computer that is targeted for remote access is unclear. From a law enforcement perspective, the cross-border unilateral application of hacking as an investigative method in these circumstances is understandable, because the use of anonymising and cloud computing services frustrates the efforts of law enforcement officials to gather evidence in cybercrime investigations. I have argued that the Dutch legislature (so far) has failed to fully recognise the sensitivity and possible political repercussions of these investigative activities. Hacking as an investigative method is very intrusive, and States are more likely to object when it is applied to computers located on their territory than when other investigative methods are applied. Possible reciprocal applications of the method must also be explicitly taken into consideration by both law enforcement officials and the judiciary when a decision is made to remotely access a computer to gather evidence.

However, a proportionate application of hacking as an investigative method may be desirable when the location of the computer involved cannot be reasonably determined and a suspect makes use of cloud computing. An approach that may be less controversial is to allow cross-border unilateral network searches and remote searches when the following three requirements are met: (1) the individual who is involved in the criminal investigation is located in the investigating State, (2) law enforcement officials already possess the login credentials necessary to access the computers, and (3) a warrant to perform the search has been obtained from an investigative judge (Conings & Oerlemans 2013, p. 29-30).[168] The interference with territorial sovereignty that takes place is not severe, since it is unclear where the interference occurs and which State is affected (cf. Koops & Goodwin 2014, p. 76 and Conings 2014, p. 14). An advantage of this approach is also that the legal certainty of the individuals involved is not endangered when these types of searches are conducted, as cross-border unilateral access is achieved from a computer on the investigating State's territory (which is also where the individuals involved are located). The use of policeware as an investigative method should in my view be restricted to computers located on the investigating State's territory. When the location of the computer that is about to be 'infected' with policeware is unknown, law enforcement officials should restrict the software's functionalities to localising the computer that is used by the individual in question.

9.7 Chapter conclusion

The aim of this chapter was to determine the extent to which is it desirable that the identified investigative methods are applied unilaterally across State borders. To achieve that aim, the legal implications of cross-border unilateral digital investigations in terms of sovereignty and legal certainty have been examined (RQ 5). Three steps have been taken specifically to answer the research question. The first step entailed examining the consequences of a cross-border unilateral application of the identified investigative methods. In the second step, a legal comparison of the Netherlands and the United States was conducted to illustrate how each State views the desirable restrictions for the cross-border unilateral application of the investigative methods and actually regulates each method. Based on the outcomes of these two steps, the third step involved making proposals for desirable restrictions to a cross-border unilateral application of the investigative methods from a Dutch perspective. The results of these steps are summarised below.

168 For instance, law enforcement officials can obtain these login credentials from a seized computer and then use them to gain access to a suspect's online account(s).

Step 1 – Consequences of cross-border unilateral investigations
This first step was addressed in section 9.1. The cross-border unilateral application of investigative methods can have extraterritorial effects that lead to an interference of the *territorial sovereignty* of the State involved, insofar as permission is not obtained from that State or a treaty basis is unavailable for the evidence-gathering activity. States respond differently to these interferences, depending on the intrusiveness of the investigative method that is used and factors such as past grievances with other States.

As a corollary of the territorial limitation of enforcement jurisdiction that serves to protect State sovereignty, the individuals located in a State are protected against arbitrary interferences from *foreign* law enforcement authorities in their private lives. The cross-border unilateral application of investigative methods can therefore lead to a situation in which foreign laws are applied to individuals who are located in the affected State. The foreign regulations that restrict the application of investigative methods are not accessible and not foreseeable to the individuals involved and will endanger the *legal certainty* of the individuals involved. Other actors engaged in the criminal justice system also require legal certainty about the conditions under which digital evidence-gathering activities are applied.

Step 2 – Legal comparison between the Dutch and U.S. approaches
The legal comparison that was part of the second step was conducted in sections 9.2 to 9.5. The analysis emphasised the different interpretations of the Netherlands and the United States regarding the principle of the territorial limitation of enforcement jurisdiction. Most notably, the analysis shown that the United States has previously engaged in the unilateral application of extraterritorial undercover investigative methods and data production orders. This practice is now likely sustained in the application of these investigative methods in an online context. However, there is not sufficient information is available to fully indicate the extent to which U.S. law enforcement authorities apply these digital investigative methods unilaterally across State borders.

In contrast, the Netherlands follows a more careful approach when the application of investigative methods produces extraterritorial effects. The legal comparison showed that the Netherlands views the application of the identified digital investigative methods as privacy intrusive and has regulated many of them in statutory law. In the United States, only the issuing of data production orders and hacking as an investigative method are regulated in statutory law. The gathering of publicly available online information and online undercover investigative method are regulated in internal guidelines. Citizens cannot derive any rights from these guidelines and their contents may vary depending on the U.S. law enforcement authority that is involved. Considerably stricter regulations apply to these two investigative methods in the Netherlands. Interestingly, both Dutch and U.S. law enforcement officials have engaged in cross-border unilateral hacking as an investigative method. Legislative bodies in both States also aim to regulate

cross-border unilateral hacking as an investigative method in the event that the target computer cannot be reasonably localised.

Overall, it should be observed that a discrepancy between theory and practice appears to exist. In theory, extraterritorial evidence-gathering activities are not allowed without permission from the affected State or a treaty basis for the evidence-gathering activity. In practice, however, cross-border unilateral digital evidence-gathering activities can – and do – take place. It is crucial that the reality of cross-border unilateral evidence-gathering activities in cybercrime investigations is dealt with and that thinking is developed about desirable restrictions in this regard. All States should start including the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. States should also endeavour to reach agreements with other States as to the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable.

Step 3 – Proposal for desirable restrictions

The third step, which was undertaken in section 9.6, entailed making proposals to regulate Dutch law enforcement officials' cross-border unilateral application of the investigative methods based on the relevant consequences identified. An overview of the results of that analysis, indicating to which extent the cross-border unilateral evidence gathering may be acceptable and thus the answers RQ 5 is provided in Table 9.1.

Investigative method	**Should the cross-border unilateral evidence-gathering activity be possible?**	**Recommended action**
Gathering publicly available online information	Yes, based on art. 32(a) of the Convention on Cybercrime. The practice is arguably part of international customary law.	It is preferable to regulate the application of systematic online observation in a treaty.
Data production orders issued to online service providers	Yes, insofar as the online service provider voluntarily cooperates.	It is preferable to regulate the application of unilateral data production orders to online service providers in a treaty.
Online undercover investigative methods	(1) Yes, insofar as the individual involved is located in the investigating State. (2) Yes, insofar as the location of the individual involved is unknown and the investigating State notifies the other State and either obtains permission or initiates mutual legal assistance procedures, as soon as the involved individual's location does become known.	States should refrain from online undercover investigation activities when it is clear that the individual involved is located on foreign territory. It is preferable to regulate the application of online undercover investigations in a treaty.
Hacking as an investigative method	(1) Yes, insofar as (A) the remote and network searches involve the online accounts or computers of an individual who is located in the investigating State's territory, (B) law enforcement officials already possess the login credentials necessary to remotely access computers, and (C) a warrant to perform the search has been obtained from a judge. (2) No, insofar as the computer targeted for policeware is clearly located on foreign territory. When this is not clear, the use of policeware should be restricted to localising the computer.	States should continue negotiations in order to agree on the terms under which remote access to computer systems on foreign territory is allowed.

Table 9.1: Proposed restrictions and regulations for the cross-border unilateral application of the identified digital investigative methods.

10 The way forward

In chapter 2, this study identified the digital investigative methods that law enforcement authorities commonly use to gather evidence in cybercrime investigations. The normative requirements for regulating investigative methods based on art. 8 ECHR were then identified in chapter 3. Thereafter, the desirable quality of regulations for these investigative methods based on the right to privacy was determined in chapter 4. In chapters 5 to 8, the identified investigative methods were placed within the Dutch legal framework to examine whether Dutch criminal procedural law regulates them in (1) an accessible manner, (2) a foreseeable manner, and (3) a manner that meets the desired quality of the law. Finally, the cross-border unilateral application of the identified digital investigative methods and consequences thereof for the territorial sovereignty of States and legal certainty of involved individuals were examined in chapter 9.

This chapter evaluates the outcomes of the analyses conducted in previous chapters in order to provide overarching observations concerning the study's results. These observations may aid in deciding which judicial steps should be taken to amend the legal framework that regulates the investigative methods used in cybercrime investigations in the Netherlands.

This chapter is structured as follows. Section 10.1 evaluates the challenges in investigating cybercrime. Section 10.2 then examines the Dutch legal framework with regard to the identified digital investigative methods on a domestic level, while section 10.3 evaluates the (inter)national legal framework with regard to the cross-border unilateral application of the identified digital investigative methods. Finally, a summary of the chapter's findings is presented in section 10.4.

10.1 Challenges in investigating cybercrime

As explained in chapter 2, three factors make it very challenging for law enforcement authorities to successfully gather enough evidence and prosecute the perpetrator of a cybercrime, namely (1) anonymity, (2) encryption, and (3) jurisdiction.

The challenge of anonymity requires law enforcement authorities to make significant efforts to identify a computer user and gather evidence that proves that he has committed a cybercrime. As explained in chapter 2, a combination of investigative methods may provide for the means to do so. Nonetheless, the success of a criminal investigation will depend on the circumstances of the case, the measures that an individual has taken to obscure his digital traces, and the expertise that is available to law enforce-

ment authorities and the resources they are willing to devote to identifying a suspect. The analysis of case law in chapters 5 to 8 showed that individuals can only be traced based on their IP address when they do not consistently use anonymising services and techniques to hide that address. In my view, it is very possible to commit a well-planned cybercrime without leaving any usable digital leads. Hacking as an investigative method is an intrusive instrument for overcoming the challenge of anonymity, but it may provide a solution under certain circumstances.[1] Moreover, law enforcement officials can also use online undercover investigative methods to identify cybercriminals based on their online handles. It appears that Dutch law enforcement officials are more reluctant to use these investigative methods compared to their U.S. counterparts. This may be explained by the fact that undercover investigative methods are considered as privacy intrusive in the Netherlands, whereas they are not considered as privacy intrusive investigative methods in the United States. This is also reflected by the stringent regulations for undercover investigative methods in the Netherlands.

In specific circumstances, encryption can make evidence-gathering activities significantly harder for law enforcement authorities in their criminal investigations. Individuals who consistently use the right encryption techniques can pose a significant challenge to law enforcement authorities. In practice, individuals often make mistakes in their 'operational security measures' that law enforcement officials can take advantage of. In addition, a well-prepared strategy may allow law enforcement authorities to seize a computer while a suspect is still using it. Hacking as an investigative method may also provide law enforcement officials with the ability to circumvent the challenges of encryption. The use of policeware may enable then to intercept communications before they are encrypted, secure evidence, and record login names and passwords that they can later utilise to access information.

Jurisdiction is the greatest challenge in cybercrime investigations. The fact that a suspect resides in the territory of a State that the investigating State does not have an extradition treaty with may prove to be an insurmountable obstacle for successfully prosecuting a cybercrime. A lack of priority in relation to executing legal assistance requests or a lack of competent law enforcement officials to gather digital evidence may also hamper evidence-gathering activities in cybercrime investigations. The ability to gather evidence by applying certain investigative methods unilaterally across State borders (see chapter 9) may provide law enforcement authorities the means to gather evidence on foreign territory. However, it will not necessarily enable them to successfully prosecute a foreign individual. Furthermore, as explained in chapter 9, many forms of cross-border digital evidence gathering activities still require permission of the affected State or a legal basis in a treaty in order to take place on a legitimate basis.

1 Policeware to relay back identifying information concerning the computer and network that used by the suspect is particularly interesting. See subsection 2.4.3.

Taken together, the challenges of anonymity, encryption, and jurisdiction can make cybercrime investigations and the successful prosecution of cybercriminals very challenging. As a consequence, law enforcement officials have propagated a strategy to 'disrupt' cybercrime.[2] For example, Europol's Cybercrime Centre has been actively disrupting cybercrime by dismantling botnets that criminals have used to commit cybercrime in recent years.[3] These operations are part of a strategy in which law enforcement authorities 'move from prosecution to the disruption of cybercrime'.[4] However, during these operations law enforcement authorities utilise far-reaching special investigative powers that are created for *gathering evidence* in criminal investigations in order to prosecute individuals for cybercrime. It is questionable that this goal is reached in these disruption operations. For instance, the above-mentioned dismantling of botnets often does not result in the successful prosecution of cybercriminals.

It is important to keep in mind that the powers created for law enforcement authorities in criminal procedural law are not meant to maintain public order by frustrating criminals in their operations (cf. Corstens & Borgers 2014, p. 26). Instead, these powers are intended to enable law enforcement officials to gather evidence in criminal investigations and determine whether a person is guilty or innocent of a crime, after which he is punished as deemed appropriate. When a society believes that new powers to disrupt or halt crime online should be granted to law enforcement authorities, a debate should take place and these powers should be restricted appropriately by law.

In the meantime, efforts must still be made to successfully prosecute cybercriminals. Criminal law has an important role to play in (1) providing just outcomes for perpetrators and victims of cybercrime; (2) achieving deterrence, rehabilitation, and societal reintegration aims in relation to con-

2 See Huisman et al. 2016, p. 67-68. See also, e.g., Jacobs (2012, p. 2764) and Prins (2012, p. 52), who described the practice as an effective strategy to combat cybercrime.

3 See the following Europol press releases about disrupting botnets (without mentions of arresting suspects), 'Notorious botnets infecting 2 million computers disrupted', 5 December 2013. Available at: https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted, 'Global action targeting Skylock malware', 10 July 2014. Available at: https://www.europol.europa.eu/content/global-action-targeting-shylock-malware, and 'Botnet taken down through international law enforcement cooperation', 25 February 2015. Available at: https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation (last visited on 18 May 2015).

4 John Leyden, 'Cuffing darknet-dwelling cyberscum is tricky. We'll "disrupt" crimes instead, warns top cop', *The Register*, 29 April 2014. Available at: http://www.channelregister.co.uk/2014/04/29/europol_boss_calls_for_push_to_disrupt_cybercrime/ (last visited on 18 May 2015). See also Europol 2015b, p. 12: *"While targeting high profile, high value targets such as malware developers may be beneficial, the disruptive effect of targeting either shared criminal infrastructure or the less ubiquitous actors who provide key support services, such as bulletproof hosting, may have more significant impact across a greater division of the cybercrime community and represent a more pragmatic approach for law enforcement."*

victed offenders; and (3) creating deterrence for potential perpetrators (cf. UNODC 2013, p. 170).

10.2 Updating the domestic legal framework

The analyses in chapters 5 to 8 have shown that the Dutch legislature has failed to create legislation that meets all three normative requirements of (1) accessibility, (2) foreseeability, and (3) an adequate quality of the law regarding the regulation of the identified digital investigative methods that are commonly used in cybercrime investigations.

This is a striking observation, seeing as the Dutch legislature is tasked with amending the legal framework when technological developments significantly influence the investigative methods that are used in criminal investigations.[5] Dutch law enforcement authorities have already been applying the identified investigative methods for years. However, the regulations for these investigative methods are either (1) non-existent or (2) ambiguous in their scope and the manner in which they are executed by law enforcement authorities.[6] That is a worrisome conclusion, given that the right to privacy – and ultimately the rule of law – aim to protect individuals from the arbitrary application of power by governmental authorities. The analysis has also shown that the quality of the law should be improved, though not necessarily (only) in criminal procedural law, with regard to all of the identified investigative methods in order to adequately regulate digital investigative methods.

The task ahead

The Dutch legislature has not amended the DCCP to better accommodate digital investigative methods since 2006.[7] Initiatives have recently been taken to update the legal framework, but both the Computer Crime Act III and the project 'Modernising Criminal Procedural Law' fail to take all regulations that are required for digital investigative methods into consideration.

The Computer Crime Act III correctly identifies the challenges that law enforcement authorities encounter in criminal investigations.[8] However, the belief that a new investigative power that would enable law enforcement authorities to hack computers – even abroad – is *the solution* for effectively combatting cybercrime by prosecuting individuals is naive. The Dutch legislature is currently overemphasising a single investigative method for gath-

5 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 12.

6 See also section 8.5.

7 Cf. *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 8.

8 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 8-16.

ering evidence more effectively in cybercrime investigations; other relevant investigative methods also merit its attention. This study has shown that hacking is not the only investigative method that law enforcement authorities use to overcome the challenges of anonymity, encryption, and jurisdiction to gather evidence in cybercrime investigations. The gathering of publicly available online information, the issuing of data production orders to online service providers, and the application of online undercover investigative methods are also important investigative methods that overcome these challenges and help law enforcement officials to gather digital evidence in cybercrime investigations.

The Dutch Ministry of Security and Justice plans to modernise Dutch criminal procedural law and make the DCCP 'technology independent' and 'future proof'.[9] In 2014, it even created a special YouTube video to inform Dutch citizens about how technology has changed society, using illustrations related to computers, cloud computing, and social media services.[10] However, after meticulously reviewing the modernisation plans, the only digital investigative method the legislator definitively seeks to update is computer searches.[11]

A *full review* of Dutch criminal procedural law is instead required to accordingly accommodate all investigative methods that relate to the digital evidence-gathering activities of law enforcement authorities. We cannot deny the digitalisation of investigative activities. The Dutch legislature should provide both the necessary instruments for law enforcement authorities to effectively execute their tasks *and* provide the citizens involved with adequate procedural safeguards to protect their rights and freedoms. This means that a broader review should be conducted than has been performed in this study. It is emphasised here that this study has only examined the accessibility, foreseeability, and desired procedural safeguards for the regulation of digital investigative methods in Dutch criminal procedural law. The requirements for regulating investigative methods were derived from art. 8 ECHR. A full review should also take the normative requirements that can be derived from other ECHR rights into consideration.[12] In addition, it is likely that organisational measures must be taken to enable Dutch law

9 See Rijksoverheid.nl, 'Contourennota Wetboek van Strafvordering in consultatie', 3 February 2015. Available at: https://www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering/nieuws/2015/02/03/contourennota-wetboek-van-strafvordering-in-consultatie (last visited on 30 December 2015).

10 Available at: https://www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering/inhoud/eenvoudigere-procedures-strafvordering (last visited on 30 December 2015).

11 See subsection 8.4.1. See also J.J. Oerlemans, 'Modernisering Strafvordering geldt niet voor de opsporing', *Computerrecht* 2016, no. 1, p. 1.

12 It should be noted that Ölçer (2008, p. 26) and Hirsch Ballin (2012, p. 42-62) both emphasise in their dissertations how heavily the ECtHR weighs the right to a fair trial as provided in art. 6 ECtHR when deciding on the legitimacy to use an investigative method in light of the ECHR. See also Groenhuijsen & Knigge 2002, p. 323-326 for a list of reasons why investigative methods may require detailed regulations in criminal procedural law.

enforcement authorities to utilise all possibilities for gathering digital evidence in criminal investigations in practical terms (cf. Huisman et al. 2016, p. 58).

Transparency and foreseeability

It is reiterated here that the events in the 1990s that led to the IRT affair were partially caused by the secretive use of undercover investigative methods in criminal investigations. In 1997, the special Van Traa inquiry commission eventually concluded that many of the undercover investigative methods that were being used in practice needed to be more strictly regulated and that more transparency was required in relation to the application of undercover investigative methods by the IRT teams.

Parallels can be drawn between the IRT affair from the 1990s and the current practice of digital evidence-gathering activities.[13] This study has shown that the legal basis for conducting digital investigative methods in Dutch criminal procedural law is currently often unclear. An adequate legal basis is often lacking for the identified digital investigative methods when taking into account their intrusiveness based on the right to privacy in art. 8 ECHR. However, I agree with Schermer that the regulation of digital investigative methods is not presently under a normative crisis, since the required legal framework basis is in part already there. After the IRT affair, the basis of the legal framework was created by the Act on Special Investigative Powers. Nevertheless, for the automated gathering of publicly available online information and hacking as an investigative method, new regulations should be created by the Dutch legislature. To adequately regulate the other types of gathering publicly available online information, more clarity should be provided about their scope and manner they are applied in guidelines that are created by the Public Prosecution Service. Furthermore, to adequately regulate the issuing data production orders to online service providers and online undercover operations, substantial amendments to the DCCP are required. Given the today's fast-paced technological environment in which digital investigative methods are applied in, the Dutch legislature must continually monitor whether Dutch criminal procedural law provides for a foreseeable legal framework that is also of sufficient quality in terms of protection for the individuals involved.

To monitor the application of (digital) investigative methods by Dutch law enforcement authorities, I concur with Buruma's recent suggestion to create a 'Supervisory Commission for the Dutch Police' (Buruma 2016, p. 1541). This supervisory commission could be mandated to control and evaluate the evidence-gathering activities of Dutch law enforcement authorities and to share its findings with both the Dutch Parliament and the public

13 See also B.W. Schermer, 'Digitale IRT-affaire of nieuwe opsporing?', 14 March 2012. Available at: http://webwereld.nl/security/59972-digitale-irt-affaire-of-nieuwe-opsporing-opinie (last visited on 4 May 2016).

(through published reports).[14] It could also identify needs for new regulations for investigative methods from both law enforcement and fundamental rights perspectives.

10.3 International legal framework

In chapter 2, this study showed that mutual legal assistance as a mechanism for obtaining evidence on foreign territory does not provide an adequate response to the global problem of cybercrime. I am not alone in this observation. For instance, Koops and Goodwin (2014, p. 41) state that: *"There seems to be considerable agreement, both with practitioners and with academic cyber-investigation experts, that classic mutual legal assistance is inadequate"*. An extensive report of the United Nations Office on Drugs and Crime (UNODC) on cybercrime also concluded that: *"analysis of formal and informal cooperation mechanisms is unable to find that the current global cooperation situation is sufficient"* (UNODC 2013, p. 208).

As a result of this failure of the mutual legal assistance model for cybercrime investigations, the international legal regime needs to be amended in relation to digital evidence-gathering activities. Current mutual legal assistance treaties seem to ignore the fact that law enforcement officials already gather digital evidence unilaterally across State borders. Treaty authors appear to think only in terms of a world in which law enforcement officials have to physically cross borders to gather evidence. All States should start including the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. They should also make efforts to reach agreements with other States concerning the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable.

Chapter 9 illustrated the manner in which digital investigative methods are today being applied unilaterally across State borders in a territorially partitioned legal world. The cross-border unilateral application of investigative methods on foreign territory should be allowed insofar as the investigative methods do not interfere with the territorial sovereignty of the involved States and legal certainty in an unacceptable manner. The problem is that States have different perspectives on (1) the severity of the infringements of

14 These reports can also include statistics regarding the use of special investigative powers in the Netherlands. In 2012, the former Dutch State Secretary of the Ministry of Security and Justice refused to publish statistics regarding data production orders, stating such information could harm criminal investigations and even citing national security grounds (*Aanhangsel Handelingen* II 2011/12, no. 2011Z23302 (Answer to Parliamentary questions of the El Fassed about online privacy). The argument that these statistics harm law enforcement investigations or national security was poorly motivated. See J.J. Oerlemans, 'Our government should provide statistics about online data collection', *Leiden Law Blog* 2012. Available at http://leidenlawblog.nl/articles/our-government-should-provide-statistics-about-online-data-collection (last visited on 25 November 2014).

their territorial sovereignty that occur when investigative methods are used on their territory by foreign law enforcement authorities and (2) the gravity of the privacy interferences that take place for the individuals involved in these cross-border unilateral cybercrime investigations. This was illustrated in chapter 9 through a legal comparison between the Netherlands and United States with regard to the identified investigative methods.

The danger is that a situation will arise in which law enforcement authorities from all over the world engage in cross-border unilateral evidence-gathering activities that are regulated by their own domestic laws. An unrestricted cross-border unilateral application of investigative methods is undesirable, because it may result in diplomatic tensions between States or other political repercussions and a practice that is not foreseeable to the individuals involved. A key aspect of both the right to privacy and the rule of law is that individuals can foresee the conditions under which law enforcement authorities can use governmental power to prevent and investigate crimes and in doing so interfere in their private lives.

The task ahead

The way forward is to harmonise criminal procedural laws and elaborate the conditions under which States can apply certain digital investigative methods unilaterally across State borders. States should engage in negotiations with each other to attempt to agree on the terms under which foreign law enforcement authorities can remotely gather evidence on foreign territory unilaterally, i.e., without consent or mutual legal assistance from local law enforcement authorities. This will require the development of a common understanding concerning the circumstances under which law enforcement authorities may conduct cross-border unilateral evidence-gathering activities (cf. UNODC 2013, p. 223). I prefer that the minimum safeguards derived from art. 8 ECHR are set as a standard. States must yield part of their territorial sovereignty to combat cybercrime more effectively while simultaneously providing a degree of legal certainty and protection for their citizens by agreeing to the conditions under which cross-border digital evidence activities can take place. However, this is easier said than done.

Previous initiatives to create a global cybercrime convention with an international cybercrime court have not taken root.[15] States are apparently unwilling to give up part of their territorial sovereignty to regulate how evidence can be collected on their territory in an online context (cf. Brenner 2010, p. 173). It is more realistic to aim for States agreeing on the conditions under which other States can collect evidence using network searches

15 See, e.g., Chief Judge Stein Schjølberg, 'Report of the Chairman of HLEG to ITU Secretary-General Dr. Hamadoun I. Touré', *ITU Global Cybersecurity Agenda (GCA)*, High-Level Experts Group (HLEG) 2008, p. 6-9. Available at: http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf (last visited on 25 February 2015). See also Stein Schjølberg and Solange Ghernaouti-Helie, 'A Global Treaty on Cybersecurity and Cybercrime', 2nd ed., 2011.

and data production orders on foreign territory within the Convention on Cybercrime, since negotiations are already under way for these investigative methods (cf. Koops & Goodwin 2014, p. 83). It may also be possible to create a mutual legal assistance treaty between the EU and the United States for cross-border unilateral data production orders that are issued to online service providers.[16] The Netherlands can also pursue the further harmonisation of criminal procedural powers on the EU level. Unfortunately, the harmonisation of any criminal procedural powers between EU Member States has been ignored in the most recent EU initiative on combating cybercrime.[17]

In the meantime, the Netherlands and other States should create a policy for cross-border unilateral digital evidence-gathering activities and be aware of the consequences that these investigative activities may have on both State sovereignty and the rights and freedoms of the individuals involved. Chapter 9 presented suggestions that should be considered as a first step towards developing a policy for cross-border unilateral cybercrime investigations. The details of the desirable procedures and treaty provisions must be subjected to further scientific study.

10.4 Chapter conclusion

This chapter evaluated the outcomes of the analyses in the previous chapters to provide overarching observations concerning the study's results. These observations may aid in deciding how we move forward in amending the domestic and international legal frameworks that regulate the digital investigative methods used in cybercrime investigations.

Section 10.1 emphasised how the challenges of (1) anonymity, (2) encryption, and (3) jurisdiction make it difficult for law enforcement officials to gather evidence in cybercrime investigations. The examined digital investigative methods may provide a solid overview of the instruments that law enforcement authorities can use to overcome these challenges in cybercrime investigations. It was pointed out that the special investigative powers that are created to provide instruments for gathering evidence and prosecuting cybercriminals cannot be solely be used to 'disrupt' cybercrime.

In section 10.2 it was argued that Dutch criminal procedural law requires a general overhaul if it is to adequately regulate the use of digital inves-

16 See the press release of the Council of the European Union on 9 June 2016, 'Fight against criminal activities in cyberspace: Council agrees on practical measures and next steps', in which the council concludes that action is required *"in the area of improving cooperation with service providers, through the development of a common framework (e.g. use of aligned forms and tools) with them to request specific categories of data"*. Available at: http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/ (last visited on 8 June 2016).

17 See the EU Directive 2013/40/EU about 'attacks against information systems' (2013/40/EU (L218/8) of 14 August 2013. See also subsection 2.5.2.

tigative methods. The Dutch legislature's current efforts to update criminal procedural law are insufficient. This study has shown that, in addition to hacking as an investigative power and the seizure of computers, the (1) gathering of publicly available online information, (2) undercover investigative methods, and (3) data production orders also require the attention of the Dutch legislature. A full review of Dutch criminal procedural law to accommodate digital investigative methods should also take the requirements of fundamental rights beyond art. 8 ECHR into consideration. A parallel was also drawn between the events that led to the Dutch IRT affair and the current practice of digital evidence-gathering activities. I have argued that the Dutch legislature and Public Prosecution Service should create legislation where needed and provide more clarity regarding the legal basis in criminal procedural law that is used to apply digital investigative methods.

In section 10.3, the international legal framework for the cross-border unilateral application of the identified investigative methods was evaluated. I argued that harmonisation in the cross-border unilateral application of the identified investigative methods is desirable. However, beyond the existing provisions in the Convention on Cybercrime, the results of the efforts to harmonise digital investigative methods have so far been disappointing. To both combat cybercrime effectively *and* protect the rights and freedoms of the individuals involved, States have to accept that cross-border unilateral digital evidence-gathering activities occur and need to be regulated on an international level. In the meantime, States should create their own policies for cross-border unilateral digital evidence-gathering activities and be aware of the consequences that these investigative activities may have on both State sovereignty and the rights and freedoms of the individuals involved.

11 Conclusion

This chapter aims to answer the problem statement by answering the four research questions that guided this study. The problem statement (PS) is formulated as follows.

PS: *To what extent does Dutch criminal procedural law adequately regulate the investigative methods used in (cross-border unilateral) cybercrime investigations?*

The chapter is structured as follows. In section 11.1, the first research question (RQ 1) is answered by explaining which investigative methods are commonly used in cybercrime investigations. In section 11.2, the results of the analysis of the right to privacy in relation to the identified investigative methods are presented. The second research question (RQ 2) is then answered by identifying the normative requirements for the regulation of investigative methods. This section also answers the third research question (RQ 3) by determining which quality of the law is desirable for the identified investigative methods. In section 11.3, the fourth research question (RQ 4) is answered through an overview of the results of the analysis of the Dutch legal framework with regard to the identified digital investigative methods (which is based on the three normative requirements extracted from art. 8 ECHR). The overview also incorporates the recommendations to adequately regulate the identified digital investigative methods in Dutch criminal procedural law. In section 11.4, the fifth research question (RQ 5) is answered by suggesting restrictions to the cross-border unilateral application of the identified digital investigative methods. The answers to these five research questions should provide the knowledge necessary to answer the problem statement (PS) in section 11.5. Finally, section 11.6 provides recommendations that are based on the results of this study.

11.1 Digital investigative methods

The first research question was formulated as follows.

RQ 1: *Which investigative methods are commonly used in cybercrime investigations?*

The analysis in chapter 2 has shown that law enforcement officials often follow two digital leads, namely IP addresses and online handles, to gather evidence in cybercrime investigations. These digital leads can help them to identify an individual and prove that person committed a cybercrime. How-

ever, cybercriminal investigations are seldom straightforward, due to the following three challenges that often arise: (1) anonymity, (2) encryption, and (3) jurisdiction.

Despite these challenges, law enforcement officials can use novel investigative methods to find the initial digital leads and following-up on them to gather evidence in criminal investigations with regard to cybercrime. An analysis of the investigative activities of law enforcement officials in cybercrime investigations revealed that the following investigative methods are commonly used in cybercrime investigations:

(1) gathering of publicly available online information;
(2) issuing data production orders to online service providers;
(3) applying online undercover investigative methods; and
(4) performing hacking as an investigative method.

In cybercrime investigations, law enforcement officials can gather evidence *unilaterally across State borders*. Law enforcement officials will remain in the territory of the investigating State to gather evidence, yet produce extraterritorial effects through their use of their investigative methods. The investigative methods can also be applied unilaterally, which means that no permission is obtained to gather evidence on the territory of the affected State and no authorising legal basis in a treaty is available for the evidence-gathering activity. This application of investigative methods gives rise to questions related to international law, which are addressed by RQ 5 (see section 11.4).

11.2 The right to privacy and digital investigative methods

The second research question was formulated as follows.

RQ 2: *Which normative requirements can be derived from art. 8 ECHR for the regulation of investigative methods?*

In chapter 3, the right to privacy as articulated in art. 8 ECHR was further examined to determine the normative requirements for the regulation of investigative methods. The analysis showed that the scope of protection under art. 8 ECHR is rather broad, which means that the application of many investigative methods interfere with the right privacy. Investigative methods that interfere with the right to privacy must meet the following three conditions in order to be considered legitimate under art. 8 ECHR: they must (1) have a legitimate aim, (2) be in accordance with the law, and (3) be necessary in a democratic society. In relation to the regulation of investigative methods, the second condition of being '*in accordance with the law*' is most important.

This condition of being 'in accordance with the law' requires that the regulations for investigative methods (1) be accessible, (2) be foreseeable, and (3) meet a certain quality of the law. These are considered to be the nor-

mative requirements for regulating investigative methods. The first normative requirement, namely accessibility, means that the law gives an adequate indication concerning the regulations for the use of investigative methods in a given case. The second normative requirement, foreseeability, implies that the legal framework for investigative methods prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which the investigative method is exercised. The third normative requirement, i.e., the quality of the law, means that regulations concerning investigative methods must be of sufficient quality. The ECtHR can specify the level of detail of the regulations and the minimum procedural safeguards that must be implemented in regulations concerning investigative methods that interfere with the right to privacy in this regard. Depending on the gravity of the privacy interference that takes place, the ECtHR requires more or less detailed law and procedural safeguards for regulating investigative methods. This mechanism, which is referred to as the 'scale of gravity for privacy interferences', was illustrated in Figure 3.1 in chapter 3 and has been important in determining the desired requirements for the regulation of the identified digital investigative methods. The scale of gravity also provided a tool for visualising the privacy interferences and locating them within the Dutch legal framework, which enabled the detection of misalignments between the quality of the law of current Dutch regulations and the desired quality of the law as that flows forth from art. 8 ECHR.

The third research question was formulated as follows.

RQ 3: *Which quality of the law is desirable for the identified digital investigative methods?*

Chapter 4 examined all of the identified digital investigative methods in relation to the right to privacy as articulated in art. 8 ECHR. The application of each investigative method interferes with the right to privacy in a different and specific manner. The ECtHR sets specific requirements for each method, depending on the gravity of the privacy interference that takes place. As the privacy interference becomes more intrusive, the ECtHR requires more detailed regulations and specific procedural safeguards. With regard to undercover investigative methods, the ECtHR has articulated qualitative requirements for the domestic legal frameworks of contracting States to prevent entrapment from occurring and to ensure a fair trial based on art. 6 ECHR. These requirements are such that it is possible to transpose them to requirements for the *regulation* of undercover operations. The identified normative requirements derived from art. 8 ECHR were thus still appropriate for testing the adequacy of the Dutch legal framework for undercover investigative methods.

The ECtHR interprets convention rights, including art. 8 ECHR, according to present-day standards. This is important in respect to digital investigative methods, since they can interfere with the right to privacy in new ways. The analysis in chapter 4 showed that no case law that specifically concerns the relation between art. 8 ECHR and the identified digital investigative method is available. Therefore, the *desirable* requirements for the investigative methods was formulated based on case law regarding similar 'counterpart' investigative methods and an analysis of the gravity of the privacy interference according to present-day standards and conditions. An overview of the desirable quality of the law articulated for each of the investigative methods is provided in Table 4.1 in chapter 4.

11.3 Regulating digital investigative methods

The fourth research question was formulated as follows.

RQ 4: *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate the identified investigative methods?*

In chapters 5 to 8, the Dutch legal framework that regulates the identified digital investigative methods was tested against the normative requirements in art. 8 ECHR. This assessment helped to detect misalignments between the Dutch legal framework and the normative requirements based on art. 8 ECHR. The results of the assessment were then used to formulate recommendations for improvements in relation to all of the identified digital investigative methods. The results of the assessment of the Dutch legal framework based on the normative requirements and an overview of the recommendations is presented below in table 11.1.

Investigative method	**Accessibility**	**Foreseeability**	**Quality of the law**	**Recommendations**
1. *Gathering publicly available online information* A. Manual gathering of publicly available online information B. Automated gathering of publicly available online information C. Observing online behaviours of individuals	A. ✓ B. ✓ C. ✓	A. ✗ B. ✗ C. ✗	A. ✓ B. ✗ C. ✗	(1) Create a guideline for the manual gathering of publicly available online information. (2) Create detailed regulations (in statutory law) for the automated gathering of publicly available online information. (3) Create a guideline for the observation of online behaviours of individuals or amend the special investigative power for systematic observation.
2. *Issuing data production orders to online service providers* A. Subscriber data B. Traffic data C. Other data D. Content data	A. ✓ B. ✓ C. ✓ D. ✓	A. ✗ B. ✗ C. ✗ D. ✗	A. ✓ B. ✗ C. ✗ D. ✗	(1) Merge the dual regime for data production orders into a single regime. (2) Clearly define each category of data in lower regulations. (3) Introduce a warrant requirement for obtaining traffic and other data.
3. *Applying online undercover investigative methods* A. Online pseudo-purchases B. Online undercover interactions C. Online infiltration operations	A. ✓ B. ✓ C. ✓	A. ✓ B. ✗ C. ✓	A. ✓ B. ✗ C. ✗	(1) Amend the special investigative power for online pseudo-purchases by removing redundant text. (2) Amend the special investigative power for systematic information gathering to better reflect it incorporates undercover interactions as an investigative method. (3) Amend the special investigative powers for systematic information gathering and infiltration by incorporating the mandatory supervision of an investigative judge.
4. *Performing hacking as an investigative method* A. Network searches B. Remote searches C. The use of policeware	A. ✓ B. ✓ C. ✓	A. ✗ B. ✗ C. ✗	A. ✓ B. ✗ C. ✓	(1) Amend the special investigative power for network searches and include with a warrant requirement. (2) Create a new special investigative power for remotely accessing computers as an investigative method, which includes the power to perform remote searches and use policeware. (3) Restrict the scope of this investigative power and create an exhaustive list of functionalities for policeware.

Table 11.1: An overview of the research results of chapters 5, 6, 7, and 8 (✓ = adequate, ✗ = not adequate).

Table 11.1 illustrates that the first normative requirement of accessibility did not prove to be problematic for the Dutch legal framework. This was to be expected, as the strong legality principle in Dutch criminal procedural law ensures that a legal basis for the investigative methods is most often present in law. However, the foreseeability requirement, i.e., that the legal framework for investigative methods prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which the investigative method is exercised, turned out to be more problematic. In addition, Table 11.1 shows that many of the identified digital investigative methods do not meet the desired quality of the law. It is further examined below how (1) the foreseeability of the regulations for investigative methods and (2) the quality of the law for the identified digital investigative methods can be improved.

Improving foreseeability within the regulations for digital investigative methods

The first and most important observation is that digital investigative methods are currently not regulated in a sufficiently foreseeable manner in Dutch law.[1] The description of investigative methods in legislative history often appear outdated, hardly any case law regarding the identified digital investigative methods is available, and public guidelines often do not mention the investigative methods.

This conclusion is worrisome, since the right to privacy – and ultimately the rule of law – aim to protect individuals from the arbitrary application of power by governmental authorities. More clarity should therefore be provided with regard to the scope of the investigative methods and the manner in which Dutch law enforcement officials apply them.

The Dutch legislature and Public Prosecution Service can make the legal framework more foreseeable by creating more detailed regulations for the application of the identified investigative methods. Three avenues exist for doing so. First, insofar as an investigative method can be placed under an existing special investigative power, the Dutch legislature or Public Prosecution Service should clarify which legal basis is specifically appropriate. This approach is desirable for the following investigative methods: the observation of the online behaviours of individuals, data production orders that are issued to online service providers, and online undercover interactions with individuals. Second, insofar as an investigative method is new and (too) distinct from existing methods to be applied on existing bases, and interferes with the rights and freedoms of the individuals involved in an intrusive manner, a new special investigative power should be created. This avenue is recommended for specific types of hacking as an investigative method. Third, insofar as an investigative method is new but does not interfere with the rights and freedoms of the individuals involved in a particularly intrusive manner, detailed regulations outside of criminal procedural law may

1 With the exception of two online undercover investigative methods. See Table 11.1.

suffice. This avenue is recommended for the manual and automated gathering of publicly available online information.

In addition, the suggestion to create a supervisory commission for the Dutch Police was made in chapter 10 (cf. Buruma 2016, p. 1541). That commission could be charged with controlling and evaluating the evidence-gathering activities of Dutch law enforcement authorities. Its findings could then be reported to the Dutch Parliament and published in public reports. This commission could also identify the need for new regulations as that needs arises, from both law enforcement and fundamental rights perspectives.

Improving the quality of the law

The second observation that can be made is that the Dutch legal framework currently does not have sufficient safeguards in place with regard to specific applications of the identified investigative methods. This statement is further argued below in relation to all four methods.

Dutch law enforcement authorities should realise that they cannot have unlimited access to publicly available online information. Data protection regulations restricts the processing of publicly available information that they gather. However, the Dutch legislature or the Public Prosecution Service should create a guideline that restricts the manual gathering of online information more concretely, by specifying how the data protection regulations should be concretely fulfilled. The pre-emptive storage of personal online information is an intrusive investigative method, since information concerning individuals who have nothing to do with criminal investigations is also stored. Furthermore, the collected data can be further processed and enriched in order to gain a more intricate picture of individuals' lives. For that reason, a recommendation was made to create detailed regulations for the automated gathering of publicly available online information. The analysis also showed that the existing safeguards in the Dutch legal framework suffice for the observation of individuals' online behaviours. However, the Dutch legislator or Public Prosecution Service should create a guideline that specifies more explicitly under which conditions this investigative method can be applied and when the application of the investigative method should be considered systematic.

Detailed regulations already exist in Dutch criminal procedural law in relation to data production orders. However, it is not sufficiently clear what kind of data falls into which category (the 'What-question') and which of two regimes for data production orders applies to online service providers (the 'Who-question'). Lower regulations should specify lists of data that fall the categories of data that can be obtained with data production orders, which are regulated as special investigative powers. In addition, more safeguards – such as a warrant from an investigative judge – should be considered for data production orders with regard to traffic and other data that are issued to online service providers. The reason for this additional safeguard is that the gathering of information from the categories of traffic data

and other data are particularly intrusive investigative methods. When this investigative method is being regulated, it should be kept in mind that the collected data can be further analysed with powerful software and enriched with other data. In addition, a warrant requirement should apply for the collection of content data, including stored files that are available at online storage providers.

The Dutch legal framework for the application of undercover investigative methods arguably does not contain sufficient safeguards based on the requirements formulated by the ECtHR in case law in the context of art. 6 ECHR, which can be transposed to art. 8 ECHR requirements. The ECtHR prefers the involvement of an investigative judge to supervise undercover operations. Without such involvement, other 'adequate safeguards' must be available in domestic legal frameworks. It is unclear whether the Dutch legal framework, which only requires that a public prosecutor be involved in the application of (1) pseudo-purchases and -services, (2) systematic information gathering, and (3) infiltration as special investigative powers, currently meets the desired quality of the law. In my view, the involvement of an investigative judge should be mandatory in the regulations for (1) (online) undercover interactions with individuals and (2) (online) infiltration operations. The need for these extra safeguards can be derived from the severe interference with the right to privacy and the dangers to the integrity of criminal investigation that accompany the application of these investigative methods, as well as the high risk of entrapment involved in their application. A risk of entrapment is also present when (online) pseudo-purchases are applied. However, the application of an (online) pseudo-purchase is less privacy intrusive than the other online undercover investigative methods. The special investigative power that regulates the one-time application of (online) pseudo-purchases is therefore is sufficient quality, even though supervision of an investigative judge is not included in the special investigative power.

At the time of writing (October 2016), the Dutch legal framework does not contain sufficient safeguards for the examined applications of hacking as an investigative method. Hacking as an investigative method should be regulated by a special investigative power in the DCCP with a warrant of an investigative judge as a procedural safeguard. A special investigative power is present for a network search, but this special investigative lacks a warrant requirement as a procedural safeguard. The Dutch legislator suggests that a remote search can be applied on the legal basis to search a place in order to secure stored data on computers. However, a remote search does not take place during a search at a place in the physical world and interferes with the right to privacy in a different and more intrusive meaner than regular computer searches, since it is applied remotely and covertly. Therefore a specific provision should be created for remote searches in the DCCP with the procedural safeguard of a warrant of an investigative judge. The use of policeware is the most intrusive digital investigative method that is examined in this study. Policeware can be remotely and covertly installed

on a computer to monitor an individual's computer behaviours. The many functionalities of policeware include the ability (1) to create a backdoor for law enforcement officials to gain remote access to a computer system; (2) to determine the location of the computer and sent back identifying information about that computer to law enforcement authorities; and (3) intercept digital communications at its source and transfer those communications back to law enforcement authorities. The use of policeware requires detailed regulations statutory law and a warrant requirement that restricts the functionalities that are used and the duration that policeware can be used. The special investigative power that authorises the use of policeware meets this quality of the law, but is more limited in scope since it can only be applied insofar the functionalities of software are restricted to recording private communications.

The proposed Computer Crime Act III regulates remote searches and the use of policeware in an only partially adequate manner. The scope of the new investigative power for hacking as an investigative method is particularly broad and should be restricted more clearly in legislation.

11.4 Cross-border unilateral application of digital investigative methods

The fifth research question was formulated as follows.

RQ 5: *To what extent is it desirable and legitimate that the identified investigative methods are applied unilaterally across State borders?*

Theoretically speaking, law enforcement officials cannot mount an investigation on foreign territory without permission from the affected State(s) or authority derived from a treaty. However, in practice law enforcement officials use digital investigative methods to collect evidence on foreign territory from their own territory. They thus apply these investigative methods *unilaterally* and *across State borders*. A disparity can currently be identified with regard to the theory of the territorial limitation of enforcement jurisdiction and the cross-border unilateral application of digital investigative methods. States should start including the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. They should also make efforts to agree with other States as to the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable. Chapter 9 examined the extent to which the cross-border unilateral application of the identified investigative methods is acceptable from a Dutch perspective.

The analysis of this research question showed that one consequence of extraterritorial evidence-gathering activities is that the affected State(s) may view the practice as a violation of their territorial sovereignty. How States respond to these interferences depends on the intrusiveness of the inves-

tigative method and factors such as past grievances with other States. In addition, as a corollary of the territorial limitation of enforcement jurisdiction and State sovereignty, the individuals located in a State are protected against arbitrary interferences from *foreign* law enforcement authorities in their private lives. The cross-border unilateral application of investigative methods can therefore lead to a situation in which foreign laws are applied to individuals who are located in the affected State. The foreign regulations that restrict the application of investigative methods are not foreseeable to the individuals involved and endanger legal certainty.

In order to illustrate the different ways in which States view interferences with State sovereignty and the right to privacy when the identified investigative methods are unilaterally applied across State borders, a legal comparison was conducted between the Netherlands and the United States. The analysis ultimately led to the conclusion that cross-border unilateral digital evidence-gathering activities already take place in practice. It was argued that the international community needs to accept the reality that the Internet enables law enforcement officials to engage in cross-border evidence-gathering activities. It would be preferable for the desirable restrictions of these cross-border unilateral evidence-gathering activities to be formulated in multinational treaties. However, a question can be raised as to whether States are willing to restrict evidence-gathering activities, especially since certain digital investigative methods can be covertly applied across State borders. In addition, not all consequences of the cross-border unilateral applications of digital investigative methods are particularly serious in terms of intrusions on sovereignty and dangers to the legal certainty of the individuals involved. However, States must take political repercussions and the reciprocal effects of their extraterritorial digital evidence-gathering practices into account. For that reason, States must formulate their own policies for cross-border unilateral digital evidence-gathering activities while waiting for appropriate multinational treaties to be concluded. Table 9.1 in chapter 9 provides an overview of the restrictions that I believe are desirable for Dutch law enforcement authorities. The debate regarding the cross-border unilateral application of digital investigative methods will hopefully be continued in the future, with States eventually negotiating international treaties that include restrictions that protect both State sovereignty and the fundamental rights and legal certainty of the individuals involved in cybercrime investigations.

11.5 Answering the problem statement

The problem statement (PS) of this study was formulated as follows.

PS: *To what extent does Dutch criminal procedural law adequately regulate the investigative methods used in (cross-border unilateral) cybercrime investigations?*

In the Netherlands, investigative methods that are used in criminal investigations are regulated in criminal procedural law. As the point of departure in the Special Investigative Powers Act, only those investigative methods that (1) interfere with the involved individuals' right to rights and freedoms in more than a minor way or (2) endanger the integrity of criminal investigations are regulated in detail. As a general principle, the Dutch legislature has stated that the regulations for investigative methods apply both 'offline' and 'online'.

However, this study has shown that a considerable degree of ambiguity exists with regard to (the interpretation of) the regulations for investigative methods in an online context. The detailed regulations for special investigative methods, which often form the counterparts for digital investigative methods and accompanying explanatory memoranda were originally written for application of the methods in the physical world. At the time when the bulk of the regulations for special investigative methods were implemented in Dutch criminal procedural law, i.e., in 1999, the Dutch legislature could also not have foreseen the implications that computers and the Internet would have for the evidence gathering activities by law enforcement officials. The Dutch legislator updated the Dutch legal framework to enable these authorities to gather evidence using data production orders and to combat cybercrime more effectively with the Computer Crime Act II. Despite these legislative efforts, ambiguity remains with regard to scope of all of the identified digital investigative methods and the manner in which they are applied. Hardly any case law is available concerning the application of digital investigative methods. In order words, the Dutch legal framework is not sufficiently foreseeable with regard to digital investigative methods. In addition, the analysis has shown that not all regulations for digital investigative methods meet the desirable quality of the law and have an adequate basis for their cross-border unilateral application.

Therefore, Dutch criminal procedural currently does not adequately regulate investigative methods that are used in cross-border unilateral cybercrime investigations. In this study, suggestions have been made to improve the foreseeability and the quality of the law for the following digital investigative methods: (1) gathering publicly available online information, (2) issuing data production orders to online service providers, (3) applying online undercover investigative methods, and (4) performing hacking as an investigative method. These suggestions are based on the normative requirements that were derived from art. 8 ECHR.

This study has also shown that amending the Dutch legal framework with regard to criminal procedural law will not be enough to adequately regulate digital investigative methods. Dutch criminal procedural law alone cannot sufficiently regulate the investigative methods that are used in cross-border unilateral cybercrime investigations, given that the *international dimension* of digital evidence-gathering activities must be taken into consideration. Amendments to the international legal framework are required. However, a significant hurdle must first be cleared. Most legal scholars who

specialise in international co-operation in criminal justice matters currently fail to see that investigative methods can be applied unilaterally across State borders in an online context. Furthermore, the current legal framework that regulates the extraterritorial evidence-gathering activities of law enforcement officials seems to assume that these officials must still physically cross a State border to gather evidence. The Internet allows for a cross-border application of investigative methods and does not take into consideration the borders of a territorially divided legal world.

The first step is thus to accept that the cross-border unilateral application of digital investigative methods is currently occurring. The second step is to amend the legal framework to allow for the cross-border application of digital investigative methods *to a certain extent*. The amended legal framework should take into account the (1) sovereignty interests of States and (2) the rights and freedoms of the individuals involved, more specifically their legal certainty. These amendments to the international legal framework will take time. Ultimately, harmonisation of the cross-border unilateral application of digital investigative methods is necessary in order to protect both (1) State interests and (2) the rights and freedoms of the individuals involved. In the meantime, States, including the Netherlands, should develop their own policies and formulate the desirable restrictions for cross-border unilateral digital evidence-gathering activities.

11.6 Recommendations

This study has extensively analysed the Dutch legal framework for the regulation of the identified digital investigative methods. It has also examined the desirable restrictions for the cross-border unilateral application of these investigative methods. The collective results of these assessments provide the basis for the recommendations discussed hereinafter, which are divided into two groups: (1) recommendations at the domestic level and (2) recommendations at the international level.

11.6.1 Recommendations at the domestic level

On a domestic level, the Dutch legislature should have a more pro-active attitude towards regulating digital investigative methods. Technological developments occur at a fast pace and the legal framework should attempt to keep up. The analysis has shown that, currently, the examples in legislative history often appear outdated, hardly any case law regarding the identified digital investigative methods is available, and public guidelines often do not mention the investigative methods. The Dutch legislature, in discussion with law enforcement authorities and the Public Prosecution Service, should provide public guidance on the interpretation of the scope of the identified investigative methods and the manner in which they are executed. When the existing legal framework is insufficient, additional regulations

must be proposed. The specific recommendations based on the normative requirements derived from art. 8 ECHR have already been provided in section 11.3 and summarised in Table 11.1.

11.6.2 Recommendations at the international level

There is currently a mismatch between the theory of the territorial limitation of enforcement jurisdiction and the cross-border unilateral application of digital investigative methods. States should start including the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. They should also make efforts to agree with other States as to the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable. States must also formulate their own policies for cross-border unilateral digital evidence-gathering activities while taking into consideration the undesirable consequences of those activities with regard to both State sovereignty and the fundamental rights and legal certainty of the individuals involved. Table 9.1 in section 9.7 presented desirable restrictions for the identified investigative methods from a Dutch perspective. However, these proposals should be considered only as a first step towards developing a policy for cross-border unilateral cybercrime investigations. The details of the desirable procedures and treaty provisions must be subjected to further scientific study. Of course, international organisations also have an important role to play in this regard.

11.7 Concluding remarks

As a final observation, I would like to note that I have been underwhelmed by the amount of existing research concerned with (1) the regulation of digital investigative methods and (2) the cross-border unilateral application of (digital) investigative methods that produce extraterritorial effects. These two developments present legal scholars with fascinating and urgent questions that are currently not being sufficiently addressed.

In practice, technically skilled individuals are experimenting with technologies and evidence-gathering methodologies that can seriously endanger the rights and freedoms of the individuals involved. However, as many IT lawyers are acutely aware of and have undoubtedly advised many times: what is possible technically is not always possible legally.

I therefore end this study with a call for legal scholars in all pertinent legal fields to learn more about IT and evaluate the implications of technological developments on our society. A basic understanding of new technologies is indeed critical if we are to accommodate these technologies within our legal frameworks in an appropriate manner.

References

Abate 2011
Abate, C. (2011), 'Online-Durchsuchung, Quellen-Telekommunikationsüberwachung und die Tücke im Detail', *Datenschutz und Datensicherheit*, vol. 35, no. 2, p. 122-125.

Adelstein 2006
Adelstein, F. (2006), 'Live Forensics: Diagnosing Your System Without Killing it First', *Communications of the ACM*, vol. 49, no. 2, p. 63-66.

AIV report 2014
Adviesraad Internationale Vraagstukken (2014), 'Het Internet. Een wereldwijde vrije ruimte met begrensde rechtsmacht', no. 92.

Akandji-Kombe 2007
Akandji-Kombe, J.-F. (2007), 'Positive Rights under the European Convention on Human Rights', Human rights handbooks, no. 7, Council of Europe.

Akehurst 1974
Akehurst, M. (1974), 'Jurisdiction in International Law', *British Yearbook of International Law,* vol. 46, p. 145-257.

Asscher 2003
Asscher, L.F. (2003), *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, diss. UvA, Amsterdam: Otto Cramwinckel.

Asscher & Ekker 2003
Asscher, L.F. & Ekker, A.H. (ed.) (2003), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam: Otto Cramwinckel.

Atzoria, Ierab & Morabito 2010
Atzoria, L., Ierab, A. & Morabito, G. (2010), 'The Internet of Things: A survey', *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 54, p. 2787-2805.

Baaijens-van Geloven 2001 in: 2001
Baaijens-van Geloven, K.G.M. (2001), 'Strafvordering Groenhuijsen & Knigge en rechtshulp', p. 349-386 in: Groenhuijsen & Knigge 2001.

Bantekas 2007
Bantekas, I. (2007), 'The principle of mutual recognition in EU criminal law', *European Law Review*, vol. 32, no. 3, p. 365-385.

Bassiouni 2008
Bassiouni, M.C. (ed.) (2008), *International Criminal Law, Vol. II Multilateral and Bilateral Enforcement Mechanisms,* 3rd ed., Leiden: Martinus Nijhoff Publishers.

Beijer et al. 2004
Beijer, A., Bokhorst, R.J., Boone, M., Brants, C.H., Lindeman, J.M.W. (2004), 'De Wet bijzondere opsporingsbevoegdheden – Eindevaluatie', WODC, no. 222, Den Haag: Boom Lemma Uitgevers.

Bellia 2001
Bellia, P.L. (2001), 'Chasing Bits across Borders', *The University of Chicago Legal Forum*, p. 35-101.

Bellovin et al. 2013
Bellovin, S.M., Blaze, M., Clarke, S. & Landau, S. (2013), 'Going Bright: Wiretapping without Weakening Communications Infrastructure', *IEEE Security and Privacy*, vol. 11, no. 1, p. 62-72.

Bellovin et al. 2014a
Bellovin, S.M., Blaze, M., Clark, S. & Landau S. (2014), 'Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet', *Northwestern Journal of Technology and Intellectual Property*, vol. 12, no. 1, p. 1-65.

Bellovin et al. 2014b
Bellovin, S.M., Hutchins, R.M., Jebera, T. & Zimmeck, S. (2014), 'When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning', *New York University Journal of Law & Liberty*, vol. 8, p. 555-628.

Bernaards, Monsma & Zinn 2012
Bernaards, F., Monsma, E. & Zinn, P. (2012), 'High Tech Crime', Criminaliteitsbeeldanalyse, KLPD.

Blom 1998
Blom, T. (1998), *Drugs in het recht, recht onder druk*, diss. Erasmus University, Gouda Quint.

Blom 2007
Blom, T. (2007), 'Een ernstige inbreuk op de rechtsorde', *Delikt & Delinkwent*, vol. 58, p. 626-638.

Boek 2000
Boek, J.L.M. (2000), 'Hacken als opsporingsmethode onder de Wet BOB', *Nederlands Juristenblad*, no. 11, p. 589-593.

Boehm & Cole 2014
Boehm, F. & Cole, M.D. (2014), 'Data Retention after the Judgement of the Court of Justice of the European Union', report for the Greens/EFA Group in the European Parliament, Münster/Luxembourg, 30 June 2014.

Borgers 2012
Borgers, M.J. (2012), 'De toekomst van artikel 359a Sv', *Delikt & Delinkwent*, no. 4, p. 257-273.

Borgers 2015
Borgers, M.J. (2015), 'Normering van "lichte" opsporingsmethoden', *Delikt & Delinkwent* 2015/15.

Borgers, Duker & Stevens 2009
Borgers, M.J., Duker, M.J.A. & Stevens, L. (ed.) (2009), *Politie in beeld. Liber amicorum Jan Naeyé*, Nijmegen: Wolf Legal Publishers.

Brenner 2002
Brenner, S.W. (2002), 'Organised Cybercrime? How Cyberspace May affect the Structure of Criminal Relationships', *North Carolina Journal of Law & Technology*, vol. 4, no. 1, p. 1-50.

Brenner & Schwerha IV 2002
Brenner, S.W. & Schwerha IV, J.J. (2002), 'Transnational Evidence Gathering and Local Prosecution of International Cybercrime', *John Marshall Journal of Computer & Information Law*, vol. 10, p. 347-395.

Brenner 2010
Brenner, S.W. (2010), *Cybercrime: criminal threats from cyberspace*, California: Praeger.

Brenner 2011
Brenner, S.W. (2011), 'The Fifth Amendment, Cell Phones and Search Incident: A Response to *Password Protected*', *Iowa Law Review Bulletin*, vol. 96, p. 78-91.

Brenner 2012
Brenner, S.W. (2012), 'Law, Dissonance, and Remote Computer Searches', *North Carolina Journal of Law & Technology*, vol. 14, no. 1, p. 43-92.

Brinkhoff 2016
Brinkhoff, S. (2016), 'Big data datamining door de politie', *Nederlands Juristenblad*, vol. 20, p. 1400-1407.

Bryant et al. 2008
Bryant, R.P. et al. (2008), *Investigating Digital Crime*, Wiley-Blackwell.

Buruma 2001
Buruma, Y. (2001), *Buitengewone opsporingsbevoegdheden*, 2nd ed., Deventer: W.E.J. Tjeenk Willink.

Buruma 2016
Buruma, Y. (2016), 'De criminele homo digitalis', Nederlands Juristenblad, p. 1534-1541.

Carter 2009
Carter, D.L. (2009), 'Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies', 2nd ed., U.S. Department of Justice.

Casey 2011
Casey, E. et al. (2011), *Digital Evidence and Computer Crime*, *Forensic Science Computers and the Internet*, 3rd ed., Elsevier 2011.

Cassese 2005
Cassese, A. (ed.) (2005), *International Law*, Oxford: Oxford University Press.

Charney 1994
Charney, S. (1994), 'Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace', *Federal Bar News*, vol. 41, no. 7, p. 489-494.

Chakravarty et al. 2014
Chakravarty, S., Barbera, M.V., Portokalidis, G., Polychronakis, M. & Keromyti, A.D. (2014), 'On the Effectiveness of Traffic Analysis Against Anonymity Networking Using Flow Records', working paper 2014.

Choo 2008
Choo, K.K.R. (2008), 'Organised crime groups in cyberspace: a typology', *Trends in Organized Crime*, vol. 11, no. 3, p. 270-295.

Ciancaglini et al. 2013
Ciancaglini, V., Balduzzi, M., Goncharov, M. & McArdle, R. (2013), 'Deepweb and Cybercrime. It's Not All About TOR', Trend Micro.

Clarke et al. 2001
Clarke, I., Sandberg, O., Wiley, B. & Hong, T.W. (2001), 'Freenet: a distributed anonymous information storage and retrieval system', in: *Designing Privacy Enhancing Technologies*, pp. 46-66, Springer Berlin Heidelberg.

Clarke et al. 2010
Clarke, I., Sandberg, O., Toseland, M., & Verendel, V. (2010), 'Private Communication Through a Network of Trusted Connections: The Dark Freenet', paper submitted to PET.

Clayton 2004
Clayton, R. (2004), 'Anonymity and traceability in cyberspace', diss. Cambridge, 2004.

Clough 2010
Clough, J. (2010), *Principles of Cybercrime*, Cambridge: Cambridge University Press.

Colarusso 2011
Colarusso, D. (2011), 'Heads in the Cloud, a Coming Storm. The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination', *Boston University Journal of Science & Technology Law*, vol. 17, p. 69-100.

Coleman 2014
Coleman, G. (2014), *Hacker, Hoaxer, Whistleblower, Spy. The Many Faces of Anonymous,* London/ New York: Verso.

Commissie Grondrechten 2000
Commissie (2000), 'Grondrechten in het digitale tijdperk', Den Haag.

Conings & Oerlemans 2013
Conings, C. & Oerlemans, J.J. (2013), 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht*, no. 1, p. 23-32.

Conings 2014
Conings, C. (2014), 'De lokalisatie van opsporing in een virtuele omgeving. Wie zoekt waar in cyberspace?', *Nullem Crimen*: Tijdschrift voor Straf-en Strafprocesrecht, no. 1, p. 1-25.

Corstens 1995
Corstens, G.J.M. (1995), 'Normatieve grenzen van opsporingsmethoden', *Delikt & Delinkwent*, vol. 25, p. 542-555.

Corstens & Groenhuijsen 2000
Corstens, G.J.M. & Groenhuijsen, M.S. (ed.) (2000), *Rede en recht: opstellen ter gelegenheid van het afscheid van Prof. mr. N. Keijzer van de Katholieke Universiteit Brabant*, Deventer: Gouda Quint.

Corstens & Borgers 2014
Corstens, G.J.M. & Borgers, M.J. (2014), *Het Nederlands strafprocesrecht*, 8th ed., Deventer: Kluwer.

Crawford (ed.) 2012
Crawford, J. (2012), *Brownlie's Principles of Public International Law,* 8th ed., Oxford: Oxford University Press.

Cryer et al. 2010
Cryer, R., Friman, H., Robinson, D., & Wilmshurst, E. (2010), *An Introduction to International Criminal Law and Procedure*, 2nd ed., Cambridge: Cambridge University Press.

CTIVD 2014
Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) (2014), 'Toezichtsrapport inzake onderzoek door de AIVD op sociale media', no. 39.

De Melai & Groenhuijsen 2008
Melai, A.L. & Groenhuijsen, M.S. (ed.) (2008), *Wetboek van Strafvordering*, Deventer: Kluwer.

De Graaf, Shosha & Gladyshev 2012
Graaf, D. de, Shosha, A.F. & Gladyshev, P. (2012), 'BREDOLAB: Shopping in the Cybercrime Underworld', research paper 2012.

De Hert 2005
De Hert, P.J.A. (2005), 'Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11', *Utrecht Law Review*, vol. 1, no. 1, p. 68-98.

De Hert & Boulet 2012
De Hert, P.J.A. & Boulet, G. (2012), 'De Yahoo-saga: de keuze tussen nationale opsporingsmethoden en internationale rechtshulpinstrumenten', *Computerrecht*, no. 5, p. 324-331.

De Schepper & Verbruggen 2013
De Schepper, K. & Verbruggen, F. (2013), 'Ontsnappen *space invaders* aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elekronische dienstverleners', *Tijdschrift voor Strafrecht*, no. 3, p. 143-166.

De Schutter 2006
De Schutter, O.E. (2006), 'Globalization and jurisdiction: Lessons from the European Convention on Human Rights', *Baltic Yearbook of International Law Online*, vol. 6, no. 1, p. 185-247.

De Smet 1999
De Smet, B. (1999). *Internationale samenwerking in strafzaken tussen Angelsaksische en continentale landen; een studie over breuken tussen accusatoire en inquisitoire processtelsels bij de uitlevering, kleine rechtshulp en overdracht van strafvervolging*, diss. Antwerpen, Antwerpen-Groningen: Intersentia Rechtswetenschappen.

Diesfeldt & De Graaf 2015
Diesfeldt, A.C. & Graaf, F.C.W. de (2015), 'Dataretentie, een kwestie van alles of niets?', *Nederlands Juristenblad*, no. 12, p. 740-747.

Diffie & Landau 2007
Diffie, W. & Landau S. (2007), *Privacy on the Line*. *The Politics of Wiretapping and Encryption Updated and Expanded Edition*, Massachusetts/London: The MIT Press.

Dingledine, Mathewson, & Syverson 2004
Dingledine, R., Mathewson, N. & Syverson, P. (2004), 'Tor: The second-generation onion router', Naval Research Lab Washington DC.

Dittrich 2012
Dittrich, D. (2012), 'So you want to take over a botnet…', LEET'12 Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats 2012, p. 1-8.

DoJ Manual 2009
U.S. Department of Justice (2009), 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations', Office of Legal Education & Executive Office for United States Attorneys.

Dommering 2000
Dommering, E.J. (ed.) (2000), *Informatierecht: fundamentale rechten voor de informatiesamenleving*, Amsterdam: Otto Cramwinckel.

Doyle 2012
Doyle, C. (2012), 'Extraterritorial Application of American Criminal Law', 15 February 2012, CRS Report for Congress.

Dzehtsiarou 2011
Dzehtsiarou, K. (2011), 'European Consensus and the Evolutive Interpretation of the European Convention on Human Rights', *German Law Review*, p. 1730-1745.

Eijkman & Weggemans 2012
Eijkman, Q.A.M. & Weggemans, D. (2012), 'Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?', *Security and Human Rights*, vol. 23, no. 4, p. 285-296.

Ekker 2003
Ekker, A.H. (2003), 'Publiekrechtelijke bescherming van verkeersgegevens', p. 41-58 in: Asscher & Ekker 2003.

Embregts 2003
Embregts, M.C.D. (2003), *Uitsluitsel over bewijsuitsluiting: een onderzoek naar de toelaatbaarheid van onrechtmatig verkregen bewijs in het strafrecht, het civiele recht en het bestuursrecht*, diss. Tilburg University, Deventer: Kluwer 2003.

Ericson & Haggerty 1997
Ericson, V. & Haggerty, K. (1997), *Policing the risk society*, Oxford: Clarendon Press.

Eshof et al. 2002
Eshof, G.L.M., Spronck, P.H.M., Boers, G., Verbeek, J.P.G.M. & Herik, H.J. van den (2002), *Opsporing van verborgen informatie*, ITeR, no. 56, Den Haag: Sdu Uitgever.

Etzioni 2002
Etzioni, A. (2002), 'Implications of Select New Technologies for Individual Rights and Public Safety', *Harvard Journal of Law & Technology*, vol. 15, no. 2, p. 258-290.

Europol 2014
Europol (2014), *The Internet Organised Crime Threat Assessment*, iOCTA, The Hague.

Europol 2015a
Europol (2015), *Exploring tomorrow's organised crime*, The Hague.

Europol 2015b
Europol (2015), *The Internet Organised Crime Threat Assessment*, iOCTA, The Hague.

Europol 2015c
Europol (2015c), *Child Sexual Exploitation Environmental Scan 2015*, European Cybercrime Centre and Virtual Global Taskforce, The Hague.

Evans 2006
Evans, M.D. (ed.) (2006), *International Law*, 2nd ed., Oxford: Oxford University Press.

Faber et al. 2010
Faber, W., Mostert, S., Faber, J. & Vrolijk, N. (2010), 'Phishing, Kinderporno, Advance-Fee internet Fraud', NICC / WODC.

Franzese 2009
Franzese, P.W. (2009), 'Sovereignty in Cyberspace: Can It Exist?', *Air Force Law Review*, vol. 64, p. 1-42.

Fijnaut in: Groenhuijsen & Knigge 2002
Fijnaut, C.J.C.F. (2002) 'Bedrijfsmatig georganiseerde particuliere opsporing en (het Wetboek van) Strafvordering', p. 689-749 in: Groenhuijsen & Knigge 2002.

Fijnaut & Marx in: Fijnaut & Marx 1995
Fijnaut, C.J.C.F. & Marx, G.T. (1995), 'The normalization of undercover policing in the West: Historical and contemporary perspectives', p. 1-27, in: Fijnaut & Marx 1995.

Fijnaut & Marx 1995
Fijnaut, C.J.C.F. & Marx, G.T. (ed.) (1995), *Undercover: Police surveillance in comparative perspective*, The Hague: Kluwer.

Fokkens & Kirkels-Vrijman 2009 in: Borgers, Duker & Stevens (ed.) 2009
Fokkens, J.W. & Kirkels-Vrijman, N. (2009), 'De artikelen 2 Politiewet 1993 en 141 en 142 Strafvordering als basis voor opsporingsbevoegdheden', p. 105-124, in: Borgers, Duker & Stevens 2009.

Føllesdal, Peters & Ulfstei 2013
Føllesdal, A., Peter, B., Ulfstei, G. (2013), *Constituting Europe: The European Court of Human Rights in a National, European and Global Context*, Cambridge: Cambridge University Press.

Forcese 2011
Forcese, G. (2011), 'Spies Without Borders: International Law and Intelligence Collection', *Journal of National Security Law & Policy*, vol. 5, p. 179-210.

Fox 2007
Fox, D. (2007), 'Realisierung, Grenzen und Risiken der "Online-Durchsuchung"', *Datenschutz und Datensicherheit*, vol. 31, no. 11, p. 827-834.

Franken 2004 in: Franken, Kaspersen & De Wild (2004)
Franken, H. (2004), 'Misbruik van informatie en van middelen van informatie- en communicatietechniek', p. 385-414 in: Franken, Kaspersen & De Wild 2004.

Franken, Kaspersen & De Wild 2004
Franken, H., Kaspersen, H.W.K., & Wild, A.H. de (2004), *Recht en Computer*, Deventer: Kluwer 2004.

Franken 2009
Franken, A.A. (2009), 'Proportionaliteit en subsidiariteit in de opsporing', *Delikt & Delinkwent*, no. 8, p. 79-92.

Gane & Mackarel 1996
Gane, C. & Mackarel, M. (1996), 'Admissibility of Evidence Obtained From Abroad Into Criminal Proceedings: The Interpretation of Mutual Legal Assistance Treaties and Use of Evidence Irregularly Obtained', *The European Journal of Crime Law, Criminal Law and Criminal Justice*, vol. 4, no. 2, p. 98-119.

Garland 2001
Garland, D. (2001), *The culture of control; crime and social order in contemporary society*, Oxford: Oxford University Press.

Gerards 2011
Gerards, J.H. (2011), *EVRM – Algemene leerstukken*, Den Haag: Sdu Uitgevers.

Gercke 2012
Gercke, M. (2012), 'Understanding cybercrime: phenomena, challengers and legal response', Geneva: ITU.

Gershowitz 2008
Gershowitz, A.M. (2008), 'The iPhone Meets the Fourth Amendment', *UCLA Law Review*, no. 1, p. 27-58.

Gill 2013 in: Ziolkowski 2013
Gill, T.D. (2013), 'Non-Intervention in the Cyber Context', p. 217-238, in: Ziolkowki 2013.

Global Justice Information Sharing Initiative 2013
Global Justice Information Sharing Initiative (2013), 'Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities. Guidance and Recommendations'.

Goldsmith 2001
Goldsmith, J.L. (2001), 'The Internet and the Legitimacy of Remote Cross-Borders Searches', *The University of Chicago Legal Forum*, no. 1, p. 103-118.

Goodman 2015
Goodman, M. (2015), *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*, New York: Doubleday.

Gordley in: Monateri 2012
Gordley, J. (2012), 'The functional method', in: Monateri 2012.

Greenwield 2006
Greenwield, A. (2006), *Everyware: The Dawning Age of Ubiquitous Computing*, Berkeley: New Riders.

Greer 1997
Greer, S. (1997), 'The Exception to Articles 8 to 11 of the European Convention on Human Rights', Human Rights Files no. 13, Council of Europe Publishing.

Greer 2000
Greer, S. (2000), 'The margin of appreciation: interpretation and discretion under the European Convention on Human Rights', Human Rights Files no. 17, Council of Europe Publishing.

Groenhuijsen & Knigge 2001
Groenhuijsen, M.S. & Knigge, G. (ed.) (2001), *Het vooronderzoek in strafzaken: tweede interimrapport onderzoeksproject Strafvordering 2001*, Deventer: Gouda Quint.

Groenhijsen & Knigge 2002
Groenhuijsen, M.S. & Knigge, G. (ed.) (2002), *Dwangmiddelen en rechtsmiddelen. Derde interimrapport onderzoeksproject Strafvordering 2001*, Deventer: Kluwer.

Groenhuijsen en Knigge 2004
Groenhuijsen, M.S. & Knigge, G. (ed.) (2004), *Afronding en verantwoording. Onderzoeksrapport strafvordering 2001*, Deventer: Kluwer.

Groothuis & De Jong 2010
Groothuis, M.M. & Jong, T. de (2010), 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk?', *Privacy & Informatie*, no. 6, p. 270-303.

Hagy 2007
Hagy, D.W. (2007), U.S. Department of Justice, *Investigations Involving the Internet and Computer Networks*, Reports 2007.

Harteveld et al. 2004
Harteveld, A.E., Hielkema, J., Keulen, B.F., Krabbe, H.G.M. (2004), *Het EVRM en het Nederlandse strafprocesrecht*, 3rd ed., Deventer: Kluwer.

Herzog-Evans 2010
Herzog-Evans, M. (ed.) (2010), *Transnational criminology manual*, Nijmegen: Wolf Legal Publishers.

Hes 2003 in: Asscher & Ekker 2003
Hes, R. (2003), 'Verkeersgegevens in nieuwe generaties telecommunicatiesystemen', p. 12-40 in: Asscher & Ekker 2003.

Hildebrandt & Gutwirth 2008
Hildebrandt, M. & Gutwirth, S. (2008), *Profiling the European Citizen*, Springer.

Hildebrandt 2013
Hildebrandt, M. (2013), 'Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace?', *University of Toronto Law Journal*, vol. 63, p. 196-224.

Hirsch Ballin 2012
Hirsch Ballin, M.F.H. (2012), *Anticipative Criminal Investigation. Theory and Counterterrorism Practice in the Netherlands and the United States*, diss. Utrecht, The Hague: T.M.C. Asser Press.

Hoffer 2000
Hoffer, M.D. (2000), 'A Fistful of Dollars: "Operation Casablanca" and the Impact of Extraterritorial Enforcement of United States Money Laundering Law', *Georgia Journal of International & Comparative Law,* p. 293-318.

Hofman 1995
Hofman, J.A. (1995), *Vertrouwelijke communicatie: een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, diss. Amsterdam (VU), Zwolle: W.E.J. Tjeenk Willink.

Hogben ed. 2011
Hogben, G. (ed.), Plohmann, D., Gerhards-Padilla, E. & Leder, F. (2011), 'Botnets: Detection, Measurement, Disinfection & Defence', ENISA.

Huisman et al. 2016
Huisman, S, Princen, M., Klerks, P. & Kop, N., 'Handelen naar waarheid'.

Jacobs 2012
Jacobs, B. (2012), 'Policeware', *Nederlands Juristenblad*, no. 39, p. 2761-2764

Janssen 2015
Janssen, S.L.J. (2015), 'De niet-verdachte burger in de bijzondere opsporing', *Nederlands Juristenblad*, no. 11, p. 680-684.

Jenkins 2001
Jenkins, P. (2001), *Beyond Tolerance, child pornography on the Internet*, New York: New York University Press.

Jewkes & Yar 2010
Jewkes, Y. & Yar, M. (2010), *Handbook of Internet Crime*, Collumpton: Willan Publishing.

Joh 2009
Joh, E.E. (2009), 'Breaking the Law to Enforce It: Undercover Police Participation in Crime', *Stanford Law Review*, vol. 61, p. 155-198.

Johnson & Post 1996
Johnson, D.R. & Post, D. (1996), 'Law and Borders – The Rise of Law in Cyberspace', *Stanford Law Review*, vol. 48, p. 1367-1402.

Joubert 1994
Joubert, Ch. (1994), 'Undercover Policing – A Comparative Study', *European Journal of Crime, Criminal Law and Criminal Justice*, no. 2, p. 18-38.

Kaspersen 2007 in: Koops 2007
Kaspersen, H.W.K. (2007), 'Het Cybercrime-verdrag van de Raad van Europa', in: Koops 2007.

Keulen & Knigge 2010
Keulen, B.F. & Knigge, G. (2010), *Strafprocesrecht*, Deventer: Kluwer.

Kerkhofs & Van Linthout 2013
Kerkhofs, J. & Van Linthout, P. (2013), *Cybercrime*, Brussel: Politeia.

Kerr 2004
Kerr, O.S. (2004), 'A User's Guide to the Stored Communications Act, and Legislator's Guide to Amending It', *The George Washington Law Review*, vol. 72, p. 1208-1243.

Kerr 2009
Kerr, O. S. (2009), 'The case for the third-party doctrine', *Michigan law review*, vol. 107, p. 561-601.

Kerr 2010
Kerr, O.S. (2010), *Computer Crime Law*, 2nd ed., American Casebook Series, West Academic Publishing.

Kerr 2012
Kerr, O.S. (2012), 'The Mosaic Theory and The Fourth Amendment', *Michigan law Review*, vol. 111, p. 311-354.

Kerr 2013
Kerr, O.S. (2013), 'ECPA Part 1: Lawful Access to Stored Content', 19 March 2013, Written statement for the United States House of Representatives Subcommittee on Crime, Terrorism, Homeland Security and Investigations.

Kerr 2014
Kerr, O.S. (2014), 'Katz Has Only One Step: The Irrelevance of Subjective Expectations', George Washington School Public Law and Legal Theory paper no. 2014-43.

King 2009
King, H. (2009), 'The Extraterritorial Human Rights Obligations of States', *Human Rights Law Review*, vol. 9. no. 4, p. 521-556.

Klip 1995
Klip, A.H. (1995), 'Extraterritoriale strafvordering', *Delikt & Delinkwent*, vol. 10, p. 1056-1078.

Klip 2012
Klip, A.H. (2012), *European Criminal Law. An Integrative Approach*, 2nd ed., Antwerpen: Intersentia.

Knigge & Kwakman 2001 in: Groenhuijsen & Knigge 2001
Knigge, G. & Kwakman, N.J.M. (2001), 'Het opsporingsbegrip en de normering van de opsporingstaak', p. 125-347 in: Groenhuijsen & Knigge 2001.

Koers 2001
Koers, J. (2001), *Nederland als verzoekende staat bij wederzijdse rechtshulp in strafzaken. Achtergronden, grenzen en mogelijkheden*, diss. Katholieke Universiteit Brabant, Nijmegen: Wolf Legal Publishers.

Kohl 2007
Kohl, U. (2007), *Jurisdiction and the Internet*, Cambridge: Cambridge University Press.

Koning 2012
Koning, M.E. (2012), 'Van teugelloos 'terughacken' naar 'digitale toegang op afstand'', *Privacy & Informatie*, no. 2, p. 46-52.

Kooijmans & Mevis 2013
Kooijmans, T. & Mevis, P.A.M. (2013), 'ICT in the context of criminal procedure: The Netherlands', TLS/EUR/AIDP.

Koops 2003 in: Asscher & Ekker 2003
Koops, E.J. (2003b), 'Verkeersgegevens en strafrecht: een agenda voor discussie', p. 59-92 in: Asscher & Ekker 2003.

Koops et al. 2005
Koops, E.J., Bekkers, R.N.A., Bongers, F.J. & Fijnvandraat, M. (2005), 'Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet', Tilburg: TILT & Dialogic.

Koops & Brenner (ed.) 2006
Koops, E.J. & Brenner, S.W. (ed.) (2006), *Cybercrime and Jurisdiction; A Global Survey*, IT & Law, no. 11, The Hague: T.M.C. Asser Press.

Koops 2007
Koops, E.J. (ed.) (2007), *Strafrecht & ICT*, Monografieën Recht en Informatietechnologie, no. 1, 2nd ed., Den Haag: Sdu Uitgevers 2007.

Koops & Buruma in: Koops 2007
Koops, E.J. & Buruma, Y. (2007), 'Formeel strafrecht en ICT', in: Koops 2007.

Koops 2010 in: M. Herzog-Evans 2010
Koops, E.J. (2010), 'The Internet and its opportunities for cybercrime', p. 735-754 in: Herzog-Evans (ed.) (2010).

Koops 2010
Koops, E.J. (2010), 'Tijd voor Computercriminaliteit III', *Nederlands Juristenblad* 2010, no. 38, p. 2461-2466.

Koops 2011
Koops, E.J. (2011), 'Digitale grondrechten en de Staatscommissie: op zoek naar de kern', *Tijdschrift voor constitutioneel recht*, no. 2, pp. 168-185.

Koops 2012a
Koops, E.J. (2012), 'Politieonderzoek in open bronnen op Internet. Strafvorderlijke aspecten', *Tijdschrift voor Veiligheid*, vol. 11, no. 2, p. 30-46.

Koops 2012b
Koops, E.J. (2012), 'Het decryptiebevel en het nemo-teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?', WODC, no. 305, Den Haag: Boom Lemma Uitgevers.

Koops et al. 2012a
Koops, E.J., Bodea, G. Broenink, G., Cuijpers, C.M.K.C., Kool, L. Prins, J.E.J. & Schellekens, M.H.M. (2012), 'Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools', Tilburg: TILT.

Koops et al. 2012b
Koops, E.J., Leenes, R.E., Hert, P.J.A. de & Olislaegers, S. (2012), 'Misdaad en opsporing in de wolken: Knelpunten en kansen van cloud computing voor de Nederlandse opsporing', WODC, Den Haag/Tilburg.

Koops 2013
Koops, E.J. (2013), 'Police investigations in internet open sources: Procedural-law issues', *Computer Law and Security Review*, vol. 29, no. 6, p. 654-665

Koops & Smits 2014
Koops, E.J. & Smits, J.M. (2014), *Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie*, Oisterwijk: Wolf Legal Publishers.

Koops & Goodwin 2014
Koops, E.J. & Goodwin, M.E.A. (2014), 'Cyberspace, the cloud and cross-border criminal investigation. The limits and possibilities of international law', WODC/TILT.

Krabbe in: Harteveld et al. 2004
Krabbe, H.G.M. (2004), 'De eerbiediging van het privé-leven', in: Harteveld et al. 2004.

Kreijen 2002
Kreijen, G. (2002), *State, Sovereignty, and International Governance*, Oxford: Oxford University Press.

Kruijsen 2013
Kruijsen, N.P.H. (2013), 'E-mail in de cloud: privacy in de prullenbak?', *Privacy & Informatie*, no. 1, p. 2-8.

Kruisbergen & De Jong 2010
Kruisbergen, E.W. & Jong, D. de (2010), 'Opsporen onder dekmantel, Regulering, uitvoering en resultaten van undercovertrajecten', WODC, no. 282, Boom Juridische Uitgevers.

Kruisbergen & De Jong 2012
Kruisbergen, E.W. & Jong, D. de (2012), 'Undercoveroperaties: een noodzakelijk kwaad?', heden, verleden en toekomst van een omstreden opsporingsmiddel, *Justitiële verkenningen*, vol. 38, no. 3, p. 50-67.

LaFave et al. 2009a
LaFave, W.R., Israel, J.H., King, N.J., & Kerr, O.S. (2009), *Criminal Procedure*, Fifth ed., Hornbook Series, Thomson Reuters.

LaFave et al. 2009b
LaFave, W.R., Israel, J.H., King, N.J., & Kerr, O.S. (2009), *Principles of Criminal Procedure*, 2nd ed., Concise Hornbook Series, Thomson Reuters.

Lawson & Schermers 1999
Lawson, R.A. & Schermers, H.G. (1999), *Leading Cases of the European Court of Human Rights*, 2nd ed., Nijmegen: Ars Aequi Libri.

Letsas 2013 in: Føllesdal, Peters & Ulfstei 2013
Letsas, G. (2013), 'The ECHR as a Living Instrument. Its Meaning and Legitimacy', p. 106-141 in: Føllesdal, Peters & Ulfstei 2013.

Lodder et al. 2014
Lodder, A.R., Meulen, N. van der, Wisman, T.H.A., Meij, L. & Zwinkels, C.M.M. (2014), 'Big Data, Big Consequences? Een verkenning naar privacy en big data gebruik binnen de opsporing, vervolging en rechtspraak', VU/WODC.

Lodder & Schuilenburg 2016
Lodder, A.R., & Schuilenburg, M.B. (2016), 'Politie-webcrawlers en Predictive policing', *Computerrecht*, no. 3, p. 150-154.

Lowe 2006 in: Evans 2006
Lowe V. (2006), 'Jurisdiction' in: Evans 2006.

Lukasik 2000
Lukasik, S.J. (2000), 'Protecting the global information commons', *Telecommunications Policy*, vol. 24, p. 519-531.

Maclin 1996
Maclin, T. (1996), 'Informants and the Fourth Amendment: a Reconsideration', *Washington University Law Quarterly*, vol. 74, p. 573-635.

Maier 1983
Maier, H.G. (1983), 'Interest Balancing and Extraterritorial Jurisdiction', *The American Journal of Comparative Law*, vol. 31, no. 4, p. 579-597.

Mann 1964
Mann, F.A. (1964), 'The Doctrine of Jurisdiction in International Law', Académie de Driot International, Recueil des Cours, Tome 111 de la Collection, Leiden: Sijthoff.

Mann 1984
Mann, F.A. (1984), 'The Doctrine of International Jurisdiction Revisted After Twenty Years', Académie de Driot International, Recueil des Cours, Tome 186 de la Collection, The Hague/Boston/London: Martinus Nijhoff Publishers.

Marx 1988
Marx, G.T. (1988), *Undercover. Police Surveillance in America*, London: University of California Press.

McCusker 2006
McCusker, R. (2006), 'Transnational organised cyber crime: distinguishing threat from reality', *Crime, Law and Social Change*, vol. 46, p. 257-273.

Mell & Grance 2009
Mell, P. & Grance, T. (2009), 'The NIST Definition of Cloud Computing', Version 15, 7 October 2009.

Messerschmidt 2013
Messerschmidt, J.E. (2013), 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm', *Columbia Journal of Transnational Law*, vol. 52, p. 275-324.

Mevis, Verbaan & Salverda 2016
Mevis, P.A.M., Verbaan, J.H.J., Salverda, B.A. (2016), *Onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken ten behoeve van de opsporing en vervolging van strafbare feiten*, Erasmus University/WODC.

Milanovic 2015
Milanovic, M. (2015), 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', *Harvard International Law Journal*, vol. 56, no. 1, p. 81-146.

Mitsilegas 2009
Mitsilegas, V. (2009), 'The third wave of third pillar EU criminal law: which direction for EU criminal justice', *European Law Review*, vol. 34, p. 523-560.

Monateri 2012
Monateri, P.G. (2012), *Methods of Comparative Law*, Research Handbooks in Comparative Law series, Cheltenham: Edward Elgar Publishing.

Moore & Rid 2016
Moore, D. & Rid, T. (2016), 'Cryptopolitik and the Darknet', *Survival*, vol. 58, no. 1, p. 7-38.

Nadelmann 1993
Nadelmann, E.A. (1993), *Cops across borders: the internationalization of U.S. criminal law enforcement*, Pennsylvania: The Pennsylvania State University Press.

Nadelmann 1995 in: Fijnaut & Marx 1995
Nadelmann, E.A. (1995), 'The DEA in Europe', in: Fijnaut & Marx 1995.

NIST 2014
National Institute of Standards and Technology (NIST), 'Cloud Computing Forensic Science Challenges', DRAFT NISTIR 8006, US Department of Commerce.

Nuis et al. 2004
Nuis, J.D.L. et al. (2004), *Particulier speurwerk verplicht*, Den Haag: Vermande.

Odinot et al. 2012
Odinot, G., Jong, D. de, Leij, J.B.J. van der, Poot, C.J. de, & Straalen, E.K. van (2012), 'Het gebruik van de telefoon- en Internettap in de opsporing', WODC, no. 304, Den Haag: Boom Lemma Uitgevers.

Odinot et al. 2013
Odinot, G., Jong, D. de, Bokhorst, R.J., Poot, C.J. de (2013), 'De Wet bewaarplicht telecommunicatiegegevens', WODC, Den Haag: Boom Lemma Uitgevers.

Oerlemans 2010
Oerlemans, J.J. (2010), 'Een verborgen wereld: kinderpornografie op Internet', *Tijdschrift voor Familie- en Jeugdrecht*, no. 10, p. 236-243.

Oerlemans 2011
Oerlemans, J.J. (2011), 'Hacken als opsporingsbevoegdheid', *Delikt & Delinkwent*, no. 8, p. 888-908.

Oerlemans 2012
Oerlemans, J.J. (2012), 'Mogelijkheden en beperkingen van de Internettap', *Justitiële Verkenningen*, vol. 38, no. 3, p. 20-39.

Oerlemans & Koops 2012
Oerlemans, J.J. & Koops, E.J. (2012), 'Surveilleren en opsporen in een Internetomgeving', *Justitiële Verkenningen*, vol. 38, no. 5, p. 35-49.

Oerlemans 2016
Oerlemans, J.J. (2016), 'Commentaar bij het Cybercrimeverdrag', in: Verrest & Paridaens 2016.

O'Floinn & Ormerod 2011
O'Floinn, M. & Ormerod, D. (2011), 'Social networking sites, RIPA and criminal investigations', *Criminal Law Review*, vol. 10, p. 766.

O'Keefe 2004
O'Keefe, R. (2004), 'Universal Jurisdiction. Clarifying the Basic Concept', *Journal of International Criminal Justice*, no. 2, p. 735-760.

Olson 2012
Olson, P. (2012), *We Are Anonymous*, New York: Little, Brown and Company.

Ölçer 2008
Ölçer, F.P. (2008), 'Eerlijk proces en bijzondere opsporing', diss. Leiden, Wolf Legal Publishers.

Ölçer 2014
Ölçer, F.P. (2014), 'De lokmethode bij de opsporing van grooming', *Computerrecht*, no. 1, p. 10-19.

Ölçer 2015
Ölçer, F.P. (2015), 'Modernisering van de bijzondere opsporing. Van BOB naar h(eimelijkeB)OB', *Strafblad*, no. 4, p. 298-307.

Paretti 2009
Paretti, K. (2009), 'Data Breaches: What the Underground World of Carding Reveals', *Santa Clara Computer & High Tech Law Journal*, vol. 25, no. 2, p. 375-414.

Parker 1976
Parker, D.B. (1976), *Crime by Computer*, New York: Scribner.

PC-OC (2008) 01
PC-OC (Committee of Experts on the Operation of European Conventions on Co-operation in Criminal matters) (2008) *Compilation of responses to questionnaire for the parties concerning the practical implementation of the Cybercrime Convention*, PC-OC (2008) 01, Strasbourg, 11 March 2008.

PC-OC (2009) 05
PC-OC (Committee of Experts on the Operation of European Conventions on Co-operation in Criminal matters) (2009), *Summary of the replies to the questionnaire on Mutual Legal Assistance in Computer-Related Cases*, PC-OC (2009) 05, p. 6, Strasbourg, 18 February 2009.

Petrashek 2009
Petrashek, N. (2009), 'Fourth Amendment and the Brave New World of Online Social Networking', *The Marquette Law Review*, vol. 93, p. 1495-1532.

Pfleeger 2003
Pfleeger, C.P. (2003), 'Data security', in: Ralston, Reilly & Hemmendinger (eds.) 2003.

Pirker 2013 in: Ziolkowki 2013
Pirker, B. (2013), 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', p. 189-216 in: Ziolkowki 2013.

Prins 2012
Prins, R. (2012), 'Een veilige cyberwereld vraagt nieuw denken', *Justitiële Verkenningen*, vol. 38, no. 1, p. 40-51.

Ralston, Reilly & Hemmendinger 2003
Ralston, A., Reilly, E.D. & Hemmendinger, D. (2003), *Encyclopedia of Computer Science*, 4th ed., Chichester: Wiley.

Reijntjes, Mos & Sjöcrona 2008
Reijntjes, J.M., Mos, M.R.B. & Sjöcrona, J.M. (2008), 'Wederzijdse rechtshulp', in: Borgers ed. 2008.

Ross 2004
Ross, J.E. (2004), 'Impediments to transnational cooperation in undercover policing: a comparative study of the United States and Italy', *The American Journal of Comparative Law*, vol. 52, no. 3, p. 569-624.

Ross 2007
Ross, J.E. (2007), 'The place of covert surveillance in democratic societies: A comparative study of the United States and Germany', *The American Journal of Comparative Law,* vol. 55, p. 493-579.

Ruggeri in: Ruggeri 2014
Ruggeri, S. (2014), 'Introduction to the Proposal of a European Investigation Orders: Due Process Concerns and Open Issues', in: Ruggeri 2014

Ruggeri 2014
Ruggeri, S. (2014), *Transnational Evidence and Multicultural Inquiries in Europe*, Springer.

Ryngaert 2007
Ryngaert, C. (2007), *Jurisdiction in international law. United States and European Perspectives,* diss. KU Leuven.

Ryngaert 2008
Ryngaert, C. (2008), *Jurisdiction in International Law*, Oxford/New York: Oxford University Press.

Sandee 2015
Sandee, M. (2015), *Game Over Zeus; Backgrounds on the Badguys and Backends*, Whitepaper for the U.S. Blackhat conference 2015.

Sandywell 2010 in: Jewkes & Yar 2010
Sanywell, B. (2010), 'On the globalisation of crime: the internet and new criminality' in: Jewkes & Yar 2010.

Spapens, Siesling & de Feijter 2011
Spapens, T., Siesling, M. & Feijter, E. de (2011), 'Brandstof voor de opsporing', Den Haag: Boom Juridische Uitgevers.

Schermer 2003
Schermer, B.W. (2003), *Opsporing vs. privacy in peer-to-peer netwerken*, ITeR, no. 64, Den Haag: Sdu Uitgevers.

Schermer 2010
Schermer, B.W. (2010), 'High tech crime en ambient intelligence', *Computerrecht* 2010, no. 6, p. 283-287.

Schneier 2007
Schneier, B. (2007), *Applied cryptography: protocols, algorithms, and source code in C*, John Wiley & Sons.

Schwerha IV 2015
Schwerha IV, J.J. (2015), 'Potential Changes in the Operation of U.S. Search Warrants to Obtain Extraterritorial Data', discussion paper Octopus Conference 2015.

Seitz 2005
Seitz, N. (2005), 'Transborder Search: A New Perspective in Law Enforcement?', *Yale Journal of Law & Technology*, no. 7, p. 24-50.

Semitsu 2011
Semitsu, J.P. (2011), 'From Facebook to mug shot: How the dearth of social networking privacy rights revolutionized online government surveillance', *Pace Law Review*, vol. 31, no. 1, p. 291-381.

Senden 2011
Senden, H.C.K. (2011), 'Interpretation of Fundamental Rights', diss. Leiden, School of Human Rights Research Series, vol. 46, Intersentia.

Shaw 2008
Shaw, M.M. (2008), *International Law*, 6th ed., Cambridge: Cambridge University Press.

Siemerink 2000a
Siemerink, L.A.R. (2000), *De wenselijkheid en mogelijkheid van infiltratie en pseudokoop op het internet*, ITeR, no. 30, Deventer: Kluwer.

Siemerink 2000b
Siemerink, L.A.R. (2000), 'Bob logt in: infiltratie en pseudokoop op internet', *Computerrecht*, no. 3, p. 141-147.

Siemerink 2000c
Siemerink, L.A.R. (2000), 'Zwaardmacht en het grensoverschrijdende internet', *Computerrecht*, no. 5, p. 239-245.

Simmelink 1987
Simmelink, J.B.H.M. (1987), *De rechtsstaatgedachte achter art. 1 Sv. Gedachten over de betekenis van art. 1 Sv voor het handelen van de overheid in de opsporingsfase*, Arnhem: Gouda Quint.

Sietsma 2006
Sietsma, R. (2006), Gegevensverwerking in het kader van de opsporing: toepassing van data-mining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy, diss. Leiden, Den Haag: Sdu Uitgevers.

Skinner 2014
Skinner, C.P. (2014), 'An International Law Response to Economic Cyber Espionage', *Connecticut Law Review*, vol. 46, no. 4, p. 1165-1207.

Smeets 2013
Smeets, S.F.J. (2013), 'De 'lokpuber': een mislukt experiment', *Strafblad*, no. 4, p. 332-338.

Smits 2006
Smits, A.H.H. (2006), *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen: Wolf Legal Publishers.

Snow 2002
Snow, T.G. (2002), 'The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them', *William & Mary Bill of Rights Journal*, vol. 11, p. 209-244.

Soghoian 2010
Soghoian, C. (2010), 'Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era', *Journal on Telecommunications & High Technology Law*, vol. 8, no. 2, p. 359-424.

Solove 2004
Solove, D.J. (2004), *The Digital Person, technology and privacy in the information age*, New York/London: New York University Press.

Soudijn & Zegers 2012
Soudijn, M.R.J. & Zegers, B.C.H.T. (2012), 'Cybercrime and virtual offender convergence settings', *Trends in Organised Crime*, vol. 15, p. 111-129.

Spoenle 2010
Spoenle, J. (2010), 'Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?', Council of Europe discussion paper.

Stahl 2011
Stahl, W.M. (2011), 'The Unchartered Waters of Cyberspace: Applying the Principles of International Martime Law to the Problem of Cybersecurity', *Georgia Journal of International Law*, vol. 40, p. 247-273.

Steenbruggen 2009
Steenbruggen, W.A.M. (2009), *Publieke dimensies van privé-communicatie. Een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk*, diss. Amsterdam (UvA), Amsterdam: Otto Cramwinckel.

Stessens 2000
Stessens, G. (2000), *Money Laundering: A New International Law Enforcement Model*, diss. Antwerpen, Cambridge: Cambridge University Press.

Stigall 2012
Stigall, D.E. (2012), 'International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law', *Hastings International & Comparative Law Review*, vol. 35, p. 324-382.

Stigall 2013
Stigall, D.E. (2013), 'Ungoverned Spaces, Transnational Crime, and the Prohibition on Extraterritorial Enforcement Jurisdiction in International Law', *Notre Dame Journal of International & Comparative Law*, p. 1-50.

Stol, Leukfeldt & Klap 2012
Stol, W.Ph., Leukfeldt, E.R., Klap, H. (2012), 'Cybercrime en politie', *Justitiële Verkenningen*, vol. 38, no. 1, p. 25-39.

Stol, Leukfeldt & Domenie 2013
Stol, W.Ph., Leukfeldt, E.R., & Domenie, M.M.L. (2013), 'Internet, Crime and the Police', *CPS*, no. 3, p. 59-81.

Struiksma, De Vey Mestdagh & Winter 2012
Struiksma, N., Vey Mestdagh, C.N.J. de & Winter, H.B. (2012), *De organisatie van de opsporing van cybercrime door de Nederlandse politie*, Politie & Wetenschap, Apeldoorn: Pro Facto, Groningen: Kees de Vey Mestdagh.

Stuntz 1995
Stuntz, W.J. (1995), 'Privacy's Problem and the Law of Criminal Procedure', *Michigan Law Review*, vol. 93, p. 1016-1078.

Summers et al. 2014
Summers, S., Schwarzenegger, C., Ege, G. & Young, F. (2014), *The Emergence of EU Criminal Law. Cybercrime and the Regulation of the Information Society*, Oxford/Portland: Hart Publishing.

Sussmann 1999
Sussmann, M.A. (1999), 'The Critical Challenges from international high-tech and computer-related crime at the milllennium', *Duke Journal Comparative & International Law*, vol. 9, p. 451-489.

Swire 2012
Swire, P. (2012), 'From real-time intercepts to stored records: why encryption drives the government to seek access to the cloud', *International Data Privacy Law*, vol. 2, no. 4, p. 200-206.

Swire & Ahmad 2012
Swire, P. & Ahmad, K. (2012), 'Encryption and Globalization', *Columbia Science & Technology Law Review*, vol. XIII, p. 416-481.

Tamanaha 2004
Tamanaha, B.Z. (2004), *On the rule of law: History, politics, theory*, Cambridge: Cambridge University Press.

T-CY 2012
T-CY (2012), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, 'Transborder access and jurisdiction: What are the options? Report of the Transborder Group', Strasbourg, 6 December 2012.

T-CY 2013
T-CY (2013) 30, Ad-hoc Subgroup on Transborder Access and Jurisdiction, 'Report of the Transborder Group for 2013', Strasbourg, 5 November 2013.

T-CY 2014
T-CY (2014), Guidance Note #3, 'Transborder access to data (Article 32), adopted by the 12th Plenary of the T-CY, Strasbourg, 2-3 December 2014.

UNODC 2012
United Nations Office on Drugs and Crime (2012), 'The use of the Internet for terrorist purposes'.

UNODC 2013
United Nations Office on Drugs and Crime (2013), 'Comprehensive Study on Cybercrime'.

UNODC 2014
United Nations Office on Drugs and Crime (2014), 'World Drug Report 2014'.

Vander Beken 1999
Vander Beken, T. (1999), *Forumkeuze in het internationaal strafrecht*, diss. Gent, Antwerpen-Apeldoorn: Maklu.

Van Buiten 2016
Van Buiten, N. (2016), 'De modernisering van de Wet BOB – Herinneren we ons de IRT-affaire nog?', *Delikt & Delinkwent*, vol. 3, p. 130-144.

Van Daele 2012
Van Daele, D. (2012), 'Verleden, heden en toekomst van de wederzijdse rechtshulp in strafzaken in de Europese Unie', *Strafblad*, vol. 10, no. 3, p. 216-224.

Van der Bel, van Hoorn & Pieters 2013
Van der Bel, D., van Hoorn, A.M. & Pieters, J.J.T.M. (2013), *Informatie en opsporing: handboek informatieverwerving, -verwerking en -verstrekking ten behoeve van de opsporingspraktijk*, 3rd ed., Zeist: Uitgeverij Kerckebosch.

Van der Wilt 2000
Van der Wilt, H.G. (2000), 'Onrechtmatig verkregen bewijsmateriaal en internationale rechtshulp in strafzaken: een impressie van de Amerikaanse rechtspraktijk', *Delikt & Delinkwent*, no. 2, p. 169-194.

Van Eeten & Bauer 2008
Van Eeten, M.J. & Bauer, J.M. (2008), 'Economics of Malware: Security Decisions, Incentives and Externalities', OECD Science, Technology and Industry Working Papers, no. 2008/01, Paris: OECD Publishing.

Van Sliedregt, Sjöcrona & Orie 2008
Van Sliedregt, E., Sjöcrona, J., & Orie, A. (2008), *Handboek Internationaal Strafrecht. Schets van het Europese en Internationale strafrecht*, Deventer: Kluwer.

Van Staden & Vollaard in: Kreijen et al. 2002
Van Staden, A. & Vollaard, H. (2002), 'The Erosion of State Sovereignty: Towards a Post-territorial World' in: Kreijen et al. 2002.

Van Woensel 2004
Van Woensel, A.M. (2004), 'Sanctionering van onrechtmatig verkregen bewijsmateriaal', *Delikt & Delinkwent*, no. 10, p. 119-171.

Verbeek, de Roos & van den Herik 2000
Verbeek, J.P.G.M, Roos, Th.A de & Herik, H.J. van den (2000), *Interceptie van vertrouwelijke communicatie*, ITeR, no. 35, Den Haag: Sdu Uitgevers.

Verbruggen 2014
Verbruggen, F. (2014), '"Om af te sluiten, druk op Start": zesde rechter in Belgische Yahoozaak schaart zich achter eerste', *Computerrecht*, no. 3, p. 129-140.

Verrest & Paridaens 2015
Verrest, P.A.M. & Paridaens, P.J.M.W., *Tekst & Commentaar Internationaal Strafrecht*, 6th ed., Deventer: Kluwer.

Walden 2007
Walden, I. (2007), *Computer Crimes and Digital Investigations*, Oxford: Oxford University Press.

Walden 2011
Walden, I. (2011), 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent', Queen Mary School of Law Legal Studies Research Paper.

Wall 2007
Wall, D.S. (2007), *Cybercrime The Transformation of Crime in the Information Age*, Cambridge: Polity Press.

Wiemans 2004
Wiemans, F.P.E. (2004), *Onderzoek van gegevens in geautomatiseerde werken*, diss. Tilburg, Nijmegen: Wolf Legal Publishers.

WRR 2016
WRR (2016), *Big Data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press.

Yar 2005
Yar, M. (2005), 'The Novelty of 'Cybercrime': an Assessment in Light of Routine Activity Theory', *European Journal of Criminology*, no. 2, p. 407-427.

Ziolkowski 2013
Ziolkowski, K. (ed.) (2013), 'Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy', Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Zuiderveen Borgesius & Arnbak 2015
Zuiderveen Borgesius, F.J. & Arnbak, A. (2015), 'New Data Security Requirements and the Proceduralization of Mass Surveillance Law after the European Data Retention Case', *Amsterdam Law School Legal Studies Research Paper*, University of Amsterdam: Amsterdam.

Zwenne & Mommers 2010
Zwenne, G.-J. & Mommers, L. (2010), 'Zijn foto's en beeldopnamen 'rasgegevens' in de zin van artikel 126nd Sv en artikel 18 Wbp?', *Privacy & Informatie*, no. 5, p. 237-247.

Zwenne & Simons 2014
Zwenne, G.-J. & Simons, F. (2014), 'Daar kon je op wachten: richtlijn bewaarplicht ongeldig verklaard', *Tijdschrift voor Internetrecht*, no. 3, p. 70-74.

Appendix A

List of respondents

Harm van Beek	–	Digital forensic scientist, Netherlands Forensic Institute
Ruud Elderhorst	–	Strategic specialist digital investigations
Erwin van Eijk	–	Digital forensic scientist, Netherlands Forensic Institute
Chris Groeneveld	–	(former) Team leader Dutch police, child abuse team
Petra Gruppelaar	–	Public prosecutor (The Hague region)
Bert Hubert	–	(former) Manager department of interception, Fox-IT
Alex de Joode	–	(former) Senior regulatory counsel, LeaseWeb
Jolanda de Klerk	–	Secretary, special commission of the Dutch Public Prosecution Service for infiltration operations
Erik Kuijl	–	Investigator Dutch police, child abuse team
Astrid Landman	–	(former) Secretary, special commission of the Dutch Public Prosecution Service for infiltration operations
Erik Ploegmakers	–	(former) Manager department of interception, Fox-IT
Christian Prickaerts	–	Manager forensics, Fox-IT
Pim Takkenberg	–	(former) Team leader Dutch police, Team High Tech Crime
Lodewijk van Zwieten	–	(former) National coordinating public prosecutor High Tech Crime & Telecom

Summary

The investigation of cybercrime requires law enforcement officials to use novel investigative methods to gather evidence. However, the legal basis for using digital investigative methods in Dutch criminal procedural law is often unclear. This study aims to answer the question of how the Dutch legislature can adequately regulate digital investigative methods. To achieve that aim, the following three steps are taken: (1) the investigative methods that are commonly used in cybercrime investigations are identified, (2) the extent to which Dutch criminal procedural law can adequately accommodate these investigative methods is analysed, and (3) the extent is examined to which these digital investigations methods can be applied unilaterally, i.e., without permission from a State or a treaty basis, across State borders.

Chapter 1 introduces the study's topic and provides a characterisation of the study. It also presents the problem statement, restrictions to the scope of the research, and research methodology. The problem statement (PS) is as follows.

PS: *To what extent does Dutch criminal procedural law adequately regulate the investigative methods used in (cross-border unilateral) cybercrime investigations?*

The 'adequate regulation of investigative methods' is understood as legislation that provides law enforcement authorities with the instruments to gather evidence in cybercrime investigations and citizens with a minimum level of protection against an arbitrary application of governmental power. To determine the minimum requirements for the regulation of investigative methods, the right to privacy in art. 8 ECHR is examined in relation to the regulation of digital investigative methods.

This problem statement leads to the following five research questions.

RQ 1: *Which investigative methods are commonly used in cybercrime investigations?*

RQ 2: *Which normative requirements can be derived from art. 8 ECHR for the regulation of investigative methods?*

RQ 3: *Which quality of the law is desirable for the identified digital investigative methods?*

RQ 4: *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate the identified investigative methods?*

RQ 5: *To what extent is it desirable and legitimate that the identified investigative methods are applied unilaterally across State borders?*

Chapter 2 answers RQ 1. The investigative methods are identified by examining which evidence-gathering activities take place in cybercrime investigations. These evidence-gathering activities are based on the digital leads of IP addresses and online handles. The investigative methods can also be applied unilaterally across State borders. However, these evidence-gathering activities are seldom straightforward, due to the three challenges of (1) anonymity, (2) encryption, and (3) the territorial limitation of enforcement jurisdiction in cybercrime investigations. By this principle, evidence-gathering activities by law enforcement authorities are restricted to the border of the investigating State, unless the activity is authorised by the other State involved or by a treaty basis. The study examines which investigative methods can be used to overcome the three challenges. The analysis shows that the following four digital investigative methods are commonly used in cybercrime investigations:

(1) gathering publicly available online information;
(2) issuing data production orders to online service providers;
(3) applying online undercover investigative methods; and
(4) performing hacking as an investigative method.

Chapter 3 answers RQ 2 by examining the relation between the right to privacy in art. 8 ECHR and the regulation of investigative methods. The examination shows that an important condition, namely that the privacy interference is '*in accordance with the law*', is particularly important for adequately regulating the investigative methods. The condition requires that the regulations for the investigative methods (1) are accessible, (2) are foreseeable, and (3) meet a certain quality of the law. In this study, these are considered to be the normative requirements for the regulation of investigative methods. The first normative requirement, accessibility, means that the law gives an adequate indication concerning the regulations for the use of investigative methods in a given case. The second normative requirement, foreseeability, implies that the legal framework for investigative methods prescribes with sufficient clarity the scope of the power conferred on the competent authorities and the manner in which the investigative method should be exercised. The third normative requirement, the quality of the law, means that regulations concerning investigative methods must be of sufficient quality. The ECtHR can specify the level of detail of the regulations and the minimum procedural safeguards for regulations concerning investigative methods that interfere with the right to privacy. The ECtHR requires more detailed law and procedural safeguards for regulating investigative methods, depending on the gravity of the privacy interference that takes place. This

mechanism is referred to as the 'scale of gravity for privacy interferences'. In this study, it has been important in determining the desired requirements for the regulation of the identified digital investigative methods. The scale of gravity also provides a tool for visualising the privacy interferences and for locating them within the Dutch legal framework. It contributes to the detection of misalignments between the quality of the law of current Dutch regulations and the desired quality of the law as it implied by art. 8 ECHR.

Chapter 4 answers RQ 3 by determining which specific requirements are desirable for the identified digital investigative methods. The chapter examines how the investigative methods interfere with the right to privacy and which quality of the law is desirable. The analysis shows that the application of investigative methods in a digital context often seriously interferes with an individuals' right to privacy. The reason is that it involves the analysis and storage of large amounts of personal data.

Chapters 5, 6, 7, and 8 answer RQ 4 with respect to each of the identified investigative methods. The three normative requirements are used to examine whether the Dutch legal framework is adequate for the investigative methods. The analysis shows that the Dutch legal framework is generally accessible. This can be attributed to the strong legality principle in Dutch law. The Dutch legality principle in criminal procedural law requires a legal basis for all privacy-interfering investigative methods. However, the *foreseeability* and the *quality of the law* of the Dutch legal framework for digital investigative methods often leave much to be desired.

It is important that the scope of the digital investigative methods and the manner in which they are applied are clear to the individuals involved, in order to avoid arbitrary interferences of law enforcement authorities in their private lives. Currently, a lack of foreseeability exists due to (1) the lack of indications about the scope of the investigative methods in statutory laws, (2) the often outdated examples in explanatory memoranda to legislation, and (3) the lack of case law regarding the application of the digital investigative methods. This shows an important and large task is ahead for the Dutch legislature and Public Prosecution Service. These entities should provide more clarity about the legal basis for digital investigative methods, their scope, as well as the manner in which they are applied.

In addition, the Dutch legal framework should meet the desired quality of the law. The desired quality of the law is in this study based on art. 8 ECHR. The analysis shows that the regulations that apply to the investigative methods were originally written for an application in an offline context. However, the application of investigative methods in an online context brings with different privacy interferences. The Dutch legal framework should take these changes into consideration. As a result of a more serious privacy interference, stronger procedural safeguards are suggested for regulations concerning the issuing of data production orders to online service providers, applying online undercover investigative methods, and perform-

ing hacking as an investigative method. The gathering of publicly available online information does not require detailed regulations with procedural safeguards in criminal procedural law. However, detailed regulations are suggested for the investigative method outside criminal procedural law.

Chapter 9 answers RQ 5. Mutual legal assistance treaties that facilitate the evidence-gathering activities of law enforcement authorities on foreign territory are written for a territorially partitioned legal world. The problem is that the Internet does not take these territorial borders into account and practically allows law enforcement officials to unilaterally gather evidence that is located on foreign territory. Despite the prohibition to gather evidence in this manner, the chapter aims to determine to what extent these cross-border unilateral digital evidence-gathering activities are acceptable. To achieve that aim, the negative consequences of this practice are further analysed. The analysis shows that the practices can (1) infringe on the territorial sovereignty of other States and (2) endanger the legal certainty of the individuals involved. The seriousness of the negative consequences are different for each investigative method. Therefore, in certain cases, the cross-border unilateral application of investigative methods could be acceptable to a certain extent. States should also recognise that digital evidence-gathering activities currently take place and should be prepared to regulate these activities insofar necessary. The study suggests which limitations for cross-border unilateral digital evidence-gathering activities are desirable and where additional regulations are necessary.

Chapter 10 evaluates the outcomes of the analyses regarding the domestic and international legal frameworks for digital investigative methods. The evaluation shows that updating the Dutch domestic legal framework to accommodate digital evidence-gathering activities is necessary, but in itself not sufficient. The international legal framework should also accommodate digital investigative methods. At present, States do not sufficiently recognise the urgency of amending the international legal framework and facilitating cross-border evidence-gathering activities by law enforcement officials in cybercrime investigations.

Chapter 11 answers the PS. The legal framework regulating digital investigative methods is in many respects outdated. The Dutch legislature is faced with the important task of updating criminal procedural law and adequately accommodating the identified digital investigative methods within the domestic legal framework. In the study, concrete suggestions are provided to improve the regulation of digital investigative methods based on the normative requirements derived from art. 8 ECHR. Due to the cross-border nature of both cybercrime and digital evidence-gathering activities, the international legal framework also requires an overhaul. States should first recognise that cross-border unilateral digital evidence-gathering activities are taking place. Amendments to mutual legal assistance treaties are

also needed to restrict and facilitate these cross-border evidence-gathering activities and protect both State sovereignty and the legal certainty of the individuals involved. Suggestions as to what these desirable restrictions may entail are provided for the Dutch legislature. The chapter is concluded with recommendations for the regulation of digital investigative methods on both the domestic level and the international level.

Samenvatting (Summary in Dutch)

Cybercrime onderzoeken

Opsporingsonderzoeken naar cybercrime vereisen het gebruik van nieuwe opsporingsmethoden om bewijs te verzamelen. De juridische basis voor deze opsporingsmethoden in het Nederlands strafprocesrecht is echter niet altijd helder en van voldoende kwaliteit. Deze studie heeft tot doel de vraag te beantwoorden op welke wijze de Nederlandse wetgever digitale opsporingsmethoden adequaat kan reguleren. Daartoe worden drie stappen genomen: (1) het identificeren van de opsporingsmethoden die veelal worden gebruikt in cybercrime-onderzoeken, (2) het nagaan in hoeverre deze opsporingsmethoden adequaat zijn gereguleerd in het Nederlands procesrecht, en (3) het analyseren in hoeverre deze digitale opsporingsmethoden grensoverschrijdend en unilateraal, c.q. zonder toestemming van de betrokken staat of zonder verdragsbasis, kunnen worden toegepast.

Hoofdstuk 1 introduceert het onderwerp van deze studie en zet de probleemstelling, beperkingen aan de reikwijdte van de studie, en onderzoeksmethodologie uiteen. De probleemstelling (PS) luidt als volgt.

PS: *In hoeverre regelt het Nederlands strafprocesrecht op adequate wijze opsporingsmethoden die worden gebruikt in (grensoverschrijdende unilaterale) cybercrime-onderzoeken?*

Onder het 'adequaat regelen van opsporingsmethoden' wordt in deze studie wetgeving verstaan die (1) opsporingsautoriteiten de instrumenten geeft om bewijs te verzamelen in cybercrime-onderzoeken en (2) een minimumniveau van bescherming biedt tegen de willekeurige inmenging van de overheid in het privéleven van burgers. De minimale vereisten voor regelgeving van digitale opsporingsmethoden zijn in deze studie afgeleid van het recht op privacy, zoals bedoeld in art. 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM).

De probleemstelling heeft geleid tot de volgende vijf onderzoeksvragen (OVs).

OV 1: *Welke opsporingsmethoden worden veelal gebruikt in cybercrime-onderzoeken?*

OV 2: *Welke vereisten voor regelgeving voor opsporingsmethoden kunnen uit art. 8 EVRM worden afgeleid?*

OV 3: *Welke kwaliteit van de wetgeving wordt vereist voor de geïdentificeerde digitale opsporingsmethoden?*

OV 4: *Op welke wijze kan het juridisch kader in het Nederlands strafprocesrecht worden verbeterd om de geïdentificeerde opsporingsmethoden afdoende te reguleren?*

OV 5: *In hoeverre is het wenselijk en legitiem om de geïdentificeerde digitale opsporingsmethoden unilateraal en over landsgrenzen heen toe te passen?*

Hoofdstuk 2 beantwoordt de eerste onderzoeksvraag (OV 1). De opsporingsmethoden zijn geïdentificeerd door na te gaan welke bewijsgaringsactiviteiten plaatsvinden in cybercrime-onderzoeken. Deze opsporingsactiviteiten vinden voornamelijk plaats op basis van de digitale sporen van (1) IP-adressen en (2) de online identiteit van mensen. De digitale opsporingsmethoden die worden gebruikt kunnen tevens grensoverschrijdend en op unilaterale wijze worden ingezet. De bewijsvergaringsactiviteiten zullen in de meeste gevallen echter niet soepel verlopen door de uitdagingen van (1) anonimiteit, (2) versleuteling, en (3) de territoriale beperking van handhavingsjurisdictie in cybercrime-onderzoeken. De territoriale beperking van handhavingsjurisdictie schrijft voor dat bewijsgaringsactiviteiten slechts tot de grens mogen worden toegepast, voor zover geen toestemming door de betrokken staat is gegeven en geen verdragsbasis voorhanden is. De studie zet uiteen welke opsporingsmethoden kunnen worden gebruikt om met deze uitdagingen om te gaan. Uit de analyse volgt dat de volgende opsporingmethoden vaak worden gebruikt in cybercrime-onderzoeken:

(1) het vergaren van publiekelijk toegankelijke online informatie;
(2) het vorderen van gegevens van online service providers;
(3) het toepassen van online undercover methoden; en
(4) het uitvoeren van hacken als opsporingsmethode.

Hoofdstuk 3 beantwoordt de tweede onderzoeksvraag (OV 2). In het hoofdstuk wordt de relatie onderzocht tussen het recht op privacy en de regulering van opsporingsmethoden. De belangrijkste voorwaarde uit art. 8 EVRM voor de regulering van opsporingsmethoden is dat de privacyinmenging 'bij de wet is voorzien'. Deze voorwaarde valt uiteen in de volgende drie eisen: (1) beschikbaarheid, (2) voorzienbaarheid, en (3) een zekere kwaliteit van wetgeving. De drie eisen worden 'normatieve vereisten' voor het reguleren van opsporingsmethoden genoemd. De eerste normatieve eis, die van beschikbaarheid, betekent dat er een indicatie moet zijn welke regelgeving van toepassing is voor het gebruik van een opsporingsmethode in een bepaald geval. De tweede normatieve eis, die van voorzienbaarheid, betekent dat het juridisch raamwerk voldoende helder (1) de reikwijdte van de bevoegdheid voor opsporingsautoriteiten aangeeft en (2) de manier waarop de opsporingsmethode wordt uitgevoerd beschrijft. De derde normatieve eis, de kwaliteit van wetgeving, betekent dat regelgeving voor opsporings-

methoden van voldoende kwaliteit moet zijn. Het Europees Hof voor de Rechten van de Mens (EHRM) kan het niveau van wetgeving en de minimale procedurele waarborgen voorschrijven. Deze kwaliteit van wetgeving moet worden geïmplementeerd in regelgeving voor opsporingsmethoden die een inmenging vormen aangaande het recht op privacy. Hoe zwaarder de privacyinbreuk, des te specifieker de wetgeving en meer waarborgen voor de bevoegdheden zijn vereist. Dit mechanisme, dat in de studie de 'schaal van zwaarte voor privacyinmengingen' wordt genoemd, is belangrijk geweest voor het vaststellen van de vereisten voor regelgeving van de geïdentificeerde opsporingsmethoden. De schaal van zwaarte voor privacyinmengingen visualiseert tevens de privacyinmenging en plaatst deze binnen het Nederlands juridisch kader. Het draagt daarmee bij aan het herkennen van de plekken waar het Nederlands juridisch kader niet voldoet aan de gewenste kwaliteit van wetgeving.

Hoofdstuk 4 beantwoordt de derde onderzoeksvraag (OV 3) door na te gaan welke kwaliteit van wetgeving gewenst is voor de regulering van de digitale opsporingsmethoden. Voorts is onderzocht hoe opsporingsmethoden een inmenging vormen aangaande het recht op privacy en welk niveau van wetgeving en waarborgen gewenst zijn om de betrokken individuen afdoende te beschermen. De analyse laat zien dat de toepassing van opsporingsmethoden in een digitale context vaak een zwaardere inmenging met het recht op privacy met zich meebrengen. Dit is zo vanwege de verwerking en opslag van grote hoeveelheden persoonsgegevens.

De vierde onderzoeksvraag (RQ 4) is beantwoord in hoofdstuk 5, 6, 7 en 8. De drie normatieve vereisten van (1) beschikbaarheid, (2) voorzienbaarheid, en (3) de geformuleerde gewenste kwaliteit van wetgeving zijn gebruikt om na te gaan in hoeverre het Nederlands juridisch kader digitale opsporingsmethoden adequaat reguleert. De analyse laat zien dat een juridische basis beschikbaar is, hetgeen kan worden verklaard door het Nederlandse strafvorderlijke legaliteitsbeginsel. Dit legaliteitsbeginsel vereist een juridische basis voor alle opsporingsmethoden die een inmenging vormen op de rechten en vrijheden van de betrokken individuen. De voorzienbaarheid en de kwaliteit van wetgeving voor digitale opsporingsmethoden is echter op veel plekken onvoldoende.

Een helder beeld over de reikwijdte van opsporingsmethoden en de manier waarop opsporingsmethoden worden toegepast, is belangrijk voor de betrokken individuen. Een willekeurige inmenging van opsporingsautoriteiten in het privéleven van personen wordt op deze manier voorkomen, hetgeen een kernelement is van de rechtsstaat. Op dit moment is er onvoldoende duidelijkheid over de reikwijdte van de geselecteerde opsporingsmethoden in de wet zelf, zijn de aangehaalde voorbeelden in de memorie van toelichting vaak achterhaald en er is een gebrek aan jurisprudentie. Dit laat zien hoe omvangrijk de taak is die voor de Nederlandse wetgever en het Openbaar Ministerie is weggelegd. Zij zullen meer helderheid moeten

verschaffen over de juridische basis die van toepassing is op de digitale opsporingsmethoden, de reikwijdte, en de manier waarop de opsporingsmethoden worden toegepast.

Het Nederlands juridisch raamwerk voor opsporingsmethoden zou bovendien aan de wenselijke kwaliteit van wetgeving moeten voldoen. De regels voor opsporingsmethoden zijn oorspronkelijk geschreven voor een offline context. De toepassing van deze opsporingsbevoegdheden in een online context brengt echter een andere privacyinmenging met zich mee. Hier moet het Nederlands juridisch kader op worden aangepast. Vanwege de zwaardere privacyinmenging zijn meer waarborgen vereist in regelgeving binnen het Wetboek van Strafvordering voor het vorderen van gegevens bij online service providers, online undercover opsporingsmethoden en hacken als opsporingsmethode. In de studie wordt verder betoogd dat het vergaren van publiekelijk toegankelijke online informatie beter buiten het Wetboek van Strafvordering kan worden geregeld.

Hoofdstuk 9 beantwoordt de vijfde onderzoeksvraag (OV 5). Rechtshulpverdragen faciliteren bewijsgaringsactiviteiten op buitenlands grondgebied, maar zijn geschreven voor een wereld dat op basis van landsgrenzen is verdeeld. Het probleem is dat internet geen rekening houdt met landsgrenzen en grensoverschrijdende unilaterale bewijsgaring praktisch mogelijk maakt. Ondanks het verbod op deze manier van bewijsgaren, wordt in het hoofdstuk nagegaan in hoeverre het wenselijk is dat de activiteiten toch plaatsvinden. Daartoe worden de negatieve effecten verder onderzocht. De analyse laat zien dat deze opsporingsactiviteiten kunnen leiden tot een inbreuk op de territoriale soevereiniteit van de betrokken Staten en de rechtszekerheid van de betrokken individuen in gevaar kan brengen. De mate waarin deze negatieve effecten zich voordoen verschillen echter per opsporingsmethode. In bepaalde gevallen zou een unilaterale grensoverschrijdende toepassing van digitale opsporingsmethoden tot op zekere hoogte mogelijk moeten zijn. Staten moeten daarnaast erkennen dat digitale bewijsgaringsactiviteiten reeds plaatsvinden en meer bereid moeten zijn deze opsporingsactiviteiten in internationaal verband te reguleren. Voor de Nederlandse wetgever wordt aangegeven waar de beperkingen van unilaterale grensoverschrijdende digitale opsporing mogelijk liggen en op welke plekken verdere regelgeving noodzakelijk is.

In hoofdstuk 10 zijn de uitkomsten van de voorafgaande analyse van het nationaal en internationaal juridisch kader voor het reguleren van digitale opsporingsmethoden geëvalueerd. De evaluatie laat zien dat het "updaten" van het Nederlands juridisch kader voor de regulering van digitale opsporingsmethoden noodzakelijk, maar op zichzelf niet voldoende is. Het bewijs en de verdachten bevinden zich vaak op buitenlands territorium. Om die reden moet ook rekening worden gehouden met het internationaal juridisch kader voor het gebruik van nationale digitale opsporingsmethoden. Tot op heden wordt de noodzaak door Staten onvoldoende onderkend om inter-

nationale verdragen aan te passen en op deze wijze grensoverschrijdende bewijsgaring in opsporingsonderzoeken naar cybercrime te faciliteren.

Hoofdstuk 11 geeft een antwoord op de probleemstelling (PS). Het juridisch raamwerk dat de digitale opsporing regelt, is in veel opzichten verouderd. Het is de hoogste tijd het Nederlands strafprocesrecht te vernieuwen en op die manier digitale opsporingsmethoden adequaat te reguleren. In hoofdstuk 5 tot en met 8 zijn verbeteringen voorgesteld op basis van de normatieve vereisten voor de regulering van opsporingsmethoden op grond van art. 8 EVRM. De grensoverschrijdende aard van cybercrime en de digitale bewijsgaringsactiviteiten in cybercrime-onderzoeken vereisen tevens aanpassing van het internationaal juridisch kader. In hoofdstuk 9 zijn concrete suggesties gedaan welke beperkingen in unilaterale grensoverschrijdende bewijsgaring de Nederlandse wetgever zou kunnen aanbrengen. De studie wordt afgesloten met een overzicht van de voorstellen voor de regulering van digitale opsporingsmethoden op nationaal en internationaal niveau.

Acknowledgements

Writing a PhD thesis is a journey we do not take alone. Therefore, I would like to thank the people who assisted me in completing this project.

My former colleagues at Fox-IT helped me to learn more about cybersecurity and the practice of digital investigations. Gratitude is owed in particular to Ronald Prins, who has supported me throughout all of my research and has always been available for discussion. I would also like to extend special thanks to my colleagues at eLaw, Center for Law and Digital Technologies at Leiden University. Our many brainstorming sessions – and the informal discussions we had during our Friday afternoon drinks – really helped me to develop my ideas about IT law. I found writing a PhD thesis to be a humbling experience, and I learned to listen to all of the comments and suggestions made concerning my manuscript. This feedback eventually brought my research to a higher level. Since it is not customary in Leiden to thank your PhD supervisors in the acknowledgements, I will refrain from doing so. However, suffice it to say I have become acutely aware of the indispensable role that supervisors play in developing the academic writing skills of a young legal scholar.

I am also grateful to Orin Kerr, Daniel Solove, and Susan Brenner. All three were willlling to spend time with me discussing the U.S. regulations for digital investigative methods with me during my tenure as a visiting scholar at George Washington University in Washington D.C.[1] My visits to the Dutch national high tech crime unit, the U.S. Secret Service headquarters, and the FBI headquarters also helped me to better understand the practice of cybercrime investigations.

This research would not have been possible without assistance from Lodewijk van Zwieten. The many interviews and the opportunity to conduct dossier research at the office of the Public Prosecution Service in Rotterdam significantly contributed to my research. I would also like to thank all other interview respondents for both taking the time to speak with me and sharing their knowledge and insights.

While working on this PhD thesis, I co-authored several publications with Bert-Jaap Koops, Bart Custers, Charlotte Conings, Ronald Pool, and Rolf van Wegberg. I thank you all for your cooperation and hope we can continue to research together in the future. I would also like to thank my colleagues at the Research and Document Centre (WODC) and the Dutch Defence Academy for their good company and cooperation in research.

1 My tenure here was sponsored by the Leiden University Fund and eLaw.

Finally, I would like to thank my parents and wife for supporting me in my research. My parents have provided me with love and support throughout my entire life. Eva, your love, support, and – perhaps above all – your patience have been very important to me. While I was never able to give you a realistic indication of when I would finish my dissertation, you graciously accepted the inevitable delays and low points I experienced along the way. During my PhD journey, we have gotten married and started our own family. I dedicate this work to our daughter, Violet.

Curriculum Vitae

Jan-Jaap Oerlemans (1985) studied law (IT law and criminal law) at Leiden University and the University of Amsterdam. From 2010 to 2015, he worked for Fox-IT as a researcher and legal consultant. In 2014, he started working for the Research and Documentation Centre of the Dutch Ministry of Security and Justice and in 2015 for the Dutch Defence Academy. In his professional work he focuses on cybercrime, privacy, digital investigations, and cybersecurity. Jan-Jaap conducted his PhD research at eLaw, Center for Law and Digital Technologies, and the E.M. Meijers Institute of Legal Studies of Leiden University. Via his supervisor, Jaap van den Herik, he was also affiliated with SIKS, the Dutch Research School for Information and Knowledge Systems.

See https://www.universiteitleiden.nl/en/staffmembers/jan-jaap-oerlemans for more information and a full list of publications.

SIKS dissertation series (2009-2016)

2009

1. Rasa Jurgelenaite (RUN) *Symmetric Causal Independence Models*
2. Willem Robert van Hage (VU) *Evaluating Ontology-Alignment Techniques*
3. Hans Stol (UvT) *A Framework for Evidence-based Policy Making Using IT*
4. Josephine Nabukenya (RUN) *Improving the Quality of Organisational Policy Making using Collaboration Engineering*
5. Sietse Overbeek (RUN) *Bridging Supply and Demand for Knowledge Intensive Tasks – Based on Knowledge, Cognition, and Quality*
6. Muhammad Subianto (UU) *Understanding Classification*
7. Ronald Poppe (UT) *Discriminative Vision-Based Recovery and Recognition of Human Motion*
8. Volker Nannen (VU) *Evolutionary Agent-Based Policy Analysis in Dynamic Environments*
9. Benjamin Kanagwa (RUN) *Design, Discovery and Construction of Service-oriented Systems*
10. Jan Wielemaker (UvA) *Logic programming for knowledge-intensive interactive applications*
11. Alexander Boer (UvA) *Legal Theory, Sources of Law & the Semantic Web*
12. Peter Massuthe (TU/e), Humboldt-Universitaet zu Berlin) *Operating Guidelines for Services*
13. Steven de Jong (UM) *Fairness in Multi-Agent Systems*
14. Maksym Korotkiy (VU) *From ontology-enabled services to service-enabled ontologies (making ontologies work in e-science with ONTO-SOA)*
15. Rinke Hoekstra (UvA) *Ontology Representation – Design Patterns and Ontologies that Make Sense*
16. Fritz Reul (UvT) *New Architectures in Computer Chess*
17. Laurens van der Maaten (UvT) *Feature Extraction from Visual Data*
18. Fabian Groffen (CWI) *Armada, An Evolving Database System*
19. Valentin Robu (CWI) *Modeling Preferences, Strategic Reasoning and Collaboration in Agent-Mediated Electronic Markets*
20. Bob van der Vecht (UU) *Adjustable Autonomy: Controling Influences on Decision Making*
21. Stijn Vanderlooy (UM) *Ranking and Reliable Classification*
22. Pavel Serdyukov (UT) *Search For Expertise: Going beyond direct evidence*
23. Peter Hofgesang (VU) *Modelling Web Usage in a Changing Environment*
24. Annerieke Heuvelink (VU) *Cognitive Models for Training Simulations*
25. Alex van Ballegooij (CWI) *"RAM: Array Database Management through Relational Mapping"*
26. Fernando Koch (UU) *An Agent-Based Model for the Development of Intelligent Mobile Services*
27. Christian Glahn (OU) *Contextual Support of social Engagement and Reflection on the Web*
28. Sander Evers (UT) *Sensor Data Management with Probabilistic Models*
29. Stanislav Pokraev (UT) *Model-Driven Semantic Integration of Service-Oriented Applications*
30. Marcin Zukowski (CWI) *Balancing vectorized query execution with bandwidth-optimized storage*
31. Sofiya Katrenko (UvA) *A Closer Look at Learning Relations from Text*
32. Rik Farenhorst (VU) and Remco de Boer (VU) *Architectural Knowledge Management: Supporting Architects and Auditors*
33. Khiet Truong (UT) *How Does Real Affect Affect Affect Recognition In Speech?*
34. Inge van de Weerd (UU) *Advancing in Software Product Management: An Incremental Method Engineering Approach*
35. Wouter Koelewijn (UL) *Privacy en Politiegegevens; Over geautomatiseerde normatieve informatie-uitwisseling*
36. Marco Kalz (OUN) *Placement Support for Learners in Learning Networks*
37. Hendrik Drachsler (OUN) *Navigation Support for Learners in Informal Learning Networks*
38. Riina Vuorikari (OU) *Tags and self-organisation: a metadata ecology for learning resources in a multilingual context*

39. Christian Stahl (TU/e), Humboldt-Universitaet zu Berlin) *Service Substitution – A Behavioral Approach Based on Petri Nets*
40. Stephan Raaijmakers (UvT) *Multinomial Language Learning: Investigations into the Geometry of Language*
41. Igor Berezhnyy (UvT) *Digital Analysis of Paintings*
42. Toine Bogers (UvT) *Recommender Systems for Social Bookmarking*
43. Virginia Nunes Leal Franqueira (UT) *Finding Multi-step Attacks in Computer Networks using Heuristic Search and Mobile Ambients*
44. Roberto Santana Tapia (UT) *Assessing Business-IT Alignment in Networked Organizations*
45. Jilles Vreeken (UU) *Making Pattern Mining Useful*
46. Loredana Afanasiev (UvA) *Querying XML: Benchmarks and Recursion*

2010

1. Matthijs van Leeuwen (UU) *Patterns that Matter*
2. Ingo Wassink (UT) *Work flows in Life Science*
3. Joost Geurts (CWI) *A Document Engineering Model and Processing Framework for Multimedia documents*
4. Olga Kulyk (UT) *Do You Know What I Know? Situational Awareness of Co-located Teams in Multidisplay Environments*
5. Claudia Hauff (UT) *Predicting the Effectiveness of Queries and Retrieval Systems*
6. Sander Bakkes (UvT) *Rapid Adaptation of Video Game AI*
7. Wim Fikkert (UT) *Gesture interaction at a Distance*
8. Krzysztof Siewicz (UL) *Towards an Improved Regulatory Framework of Free Software. Protecting user freedoms in a world of software communities and eGovernments*
9. Hugo Kielman (UL) *A Politiele gegevensverwerking en Privacy, Naar een effectieve waarborging*
10. Rebecca Ong (UL) *Mobile Communication and Protection of Children*
11. Adriaan Ter Mors (TUD) *The world according to MARP: Multi-Agent Route Planning*
12. Susan van den Braak (UU) *Sensemaking software for crime analysis*
13. Gianluigi Folino (RUN) *High Performance Data Mining using Bio-inspired techniques*
14. Sander van Splunter (VU) *Automated Web Service Reconfiguration*
15. Lianne Bodenstaff (UT) *Managing Dependency Relations in Inter-Organizational Models*
16. Sicco Verwer (TUD) *Efficient Identification of Timed Automata, theory and practice*
17. Spyros Kotoulas (VU) *Scalable Discovery of Networked Resources: Algorithms, Infrastructure, Applications*
18. Charlotte Gerritsen (VU) *Caught in the Act: Investigating Crime by Agent-Based Simulation*
19. Henriette Cramer (UvA) *People's Responses to Autonomous and Adaptive Systems*
20. Ivo Swartjes (UT) *Whose Story Is It Anyway? How Improv Informs Agency and Authorship of Emergent Narrative*
21. Harold van Heerde (UT) *Privacy-aware data management by means of data degradation*
22. Michiel Hildebrand (CWI) *End-user Support for Access to\\ Heterogeneous Linked Data*
23. Bas Steunebrink (UU) *The Logical Structure of Emotions*
24. Dmytro Tykhonov (TUD) *Designing Generic and Efficient Negotiation Strategies*
25. Zulfiqar Ali Memon (VU) *Modelling Human-Awareness for Ambient Agents: A Human Mindreading Perspective*
26. Ying Zhang (CWI) *XRPC: Efficient Distributed Query Processing on Heterogeneous XQuery Engines*
27. Marten Voulon (UL) *Automatisch contracteren*
28. Arne Koopman (UU) *Characteristic Relational Patterns*
29. Stratos Idreos(CWI) *Database Cracking: Towards Auto-tuning Database Kernels*
30. Marieke van Erp (UvT) *Accessing Natural History – Discoveries in data cleaning, structuring, and retrieval*
31. Victor de Boer (UvA) *Ontology Enrichment from Heterogeneous Sources on the Web*
32. Marcel Hiel (UvT) *An Adaptive Service Oriented Architecture: Automatically solving Interoperability Problems*
33. Robin Aly (UT) *Modeling Representation Uncertainty in Concept-Based Multimedia Retrieval*
34. Teduh Dirgahayu (UT) *Interaction Design in Service Compositions*
35. Dolf Trieschnigg (UT) *Proof of Concept: Concept-based Biomedical Information Retrieval*

36. Jose Janssen (OU) *Paving the Way for Lifelong Learning; Facilitating competence development through a learning path specification*
37. Niels Lohmann (TU/e) *Correctness of services and their composition*
38. Dirk Fahland (TU/e) *From Scenarios to components*
39. Ghazanfar Farooq Siddiqui (VU) *Integrative modeling of emotions in virtual agents*
40. Mark van Assem (VU) *Converting and Integrating Vocabularies for the Semantic Web*
41. Guillaume Chaslot (UM) *Monte-Carlo Tree Search*
42. Sybren de Kinderen (VU) *Needs-driven service bundling in a multi-supplier setting – the computational e3-service approach*
43. Peter van Kranenburg (UU) *A Computational Approach to Content-Based Retrieval of Folk Song Melodies*
44. Pieter Bellekens (TU/e) *An Approach towards Context-sensitive and User-adapted Access to Heterogeneous Data Sources, Illustrated in the Television Domain*
45. Vasilios Andrikopoulos (UvT) *A theory and model for the evolution of software services*
46. Vincent Pijpers (VU) *e3alignment: Exploring Inter-Organizational Business-ICT Alignment*
47. Chen Li (UT) *Mining Process Model Variants: Challenges, Techniques, Examples*
48. Withdrawn
49. Jahn-Takeshi Saito (UM) *Solving difficult game positions*
50. Bouke Huurnink (UvA) *Search in Audiovisual Broadcast Archives*
51. Alia Khairia Amin (CWI) *Understanding and supporting information seeking tasks in multiple sources*
52. Peter-Paul van Maanen (VU) *Adaptive Support for Human-Computer Teams: Exploring the Use of Cognitive Models of Trust and Attention*
53. Edgar Meij (UvA) *Combining Concepts and Language Models for Information Access*

2011

1. Botond Cseke (RUN) *Variational Algorithms for Bayesian Inference in Latent Gaussian Models*
2. Nick Tinnemeier (UU) *Organizing Agent Organizations. Syntax and Operational Semantics of an Organization-Oriented Programming Language*
3. Jan Martijn van der Werf (TU/e) *Compositional Design and Verification of Component-Based Information Systems*
4. Hado van Hasselt (UU) *Insights in Reinforcement Learning; Formal analysis and empirical evaluation of temporal-difference learning algorithms*
5. Base van der Raadt (VU) *Enterprise Architecture Coming of Age – Increasing the Performance of an Emerging Discipline.*
6. Yiwen Wang (TU/e) *Semantically-Enhanced Recommendations in Cultural Heritage*
7. Yujia Cao (UT) *Multimodal Information Presentation for High Load Human Computer Interaction*
8. Nieske Vergunst (UU) *BDI-based Generation of Robust Task-Oriented Dialogues*
9. Tim de Jong (OU) *Contextualised Mobile Media for Learning*
10. Bart Bogaert (UvT) *Cloud Content Contention*
11. Dhaval Vyas (UT) *Designing for Awareness: An Experience-focused HCI Perspective*
12. Carmen Bratosin (TU/e) *Grid Architecture for Distributed Process Mining*
13. Xiaoyu Mao (UvT) *Airport under Control. Multiagent Scheduling for Airport Ground Handling*
14. Milan Lovric (EUR) *Behavioral Finance and Agent-Based Artificial Markets*
15. Marijn Koolen (UvA) *The Meaning of Structure: the Value of Link Evidence for Information Retrieval*
16. Maarten Schadd (UM) *Selective Search in Games of Different Complexity*
17. Jiyin He (UvA) *Exploring Topic Structure: Coherence, Diversity and Relatedness*
18. Mark Ponsen (UM) *Strategic Decision-Making in complex games*
19. Ellen Rusman (OU) *The Mind's Eye on Personal Profiles*
20. Qing Gu (VU) *Guiding service-oriented software engineering – A view-based approach*
21. Linda Terlouw (TUD) *Modularization and Specification of Service-Oriented Systems*
22. Junte Zhang (UvA) *System Evaluation of Archival Description and Access*
23. Wouter Weerkamp (UvA) *Finding People and their Utterances in Social Media*
24. Herwin van Welbergen (UT) *Behavior Generation for Interpersonal Coordination with Virtual Humans On Specifying, Scheduling and Realizing Multimodal Virtual Human Behavior*
25. Syed Waqar ul Qounain Jaffry (VU) *Analysis and Validation of Models for Trust Dynamics*

26. Matthijs Aart Pontier (VU) *Virtual Agents for Human Communication – Emotion Regulation and Involvement-Distance Trade-Offs in Embodied Conversational Agents and Robots*
27. Aniel Bhulai (VU) *Dynamic website optimization through autonomous management of design patterns*
28. Rianne Kaptein (UvA) *Effective Focused Retrieval by Exploiting Query Context and Document Structure*
29. Faisal Kamiran (TU/e) *Discrimination-aware Classification*
30. Egon van den Broek (UT) *Affective Signal Processing (ASP): Unraveling the mystery of emotions*
31. Ludo Waltman (EUR) *Computational and Game-Theoretic Approaches for Modeling Bounded Rationality*
32. Nees-Jan van Eck (EUR) *Methodological Advances in Bibliometric Mapping of Science*
33. Tom van der Weide (UU) *Arguing to Motivate Decisions*
34. Paolo Turrini (UU) *Strategic Reasoning in Interdependence: Logical and Game-theoretical Investigations*
35. Maaike Harbers (UU) *Explaining Agent Behavior in Virtual Training*
36. Erik van der Spek (UU) *Experiments in serious game design: a cognitive approach*
37. Adriana Burlutiu (RUN) *Machine Learning for Pairwise Data, Applications for Preference Learning and Supervised Network Inference*
38. Nyree Lemmens (UM) *Bee-inspired Distributed Optimization*
39. Joost Westra (UU) *Organizing Adaptation using Agents in Serious Games*
40. Viktor Clerc (VU) *Architectural Knowledge Management in Global Software Development*
41. Luan Ibraimi (UT) *Cryptographically Enforced Distributed Data Access Control*
42. Michal Sindlar (UU) *Explaining Behavior through Mental State Attribution*
43. Henk van der Schuur (UU) *Process Improvement through Software Operation Knowledge*
44. Boris Reuderink (UT) *Robust Brain-Computer Interfaces*
45. Herman Stehouwer (UvT) *Statistical Language Models for Alternative Sequence Selection*
46. Beibei Hu (TUD) *Towards Contextualized Information Delivery: A Rule-based Architecture for the Domain of Mobile Police Work*
47. Azizi Bin Ab Aziz(VU) *Exploring Computational Models for Intelligent Support of Persons with Depression*
48. Mark Ter Maat (UT) *Response Selection and Turn-taking for a Sensitive Artificial Listening Agent*
49. Andreea Niculescu (UT) *Conversational interfaces for task-oriented spoken dialogues: design aspects influencing interaction quality*

2012

1. Terry Kakeeto (UvT) *Relationship Marketing for SMEs in Uganda*
2. Muhammad Umair (VU) *Adaptivity, emotion, and Rationality in Human and Ambient Agent Models*
3. Adam Vanya (VU) *Supporting Architecture Evolution by Mining Software Repositories*
4. Jurriaan Souer (UU) *Development of Content Management System-based Web Applications*
5. Marijn Plomp (UU) *Maturing Interorganisational Information Systems*
6. Wolfgang Reinhardt (OU) *Awareness Support for Knowledge Workers in Research Networks*
7. Rianne van Lambalgen (VU) *When the Going Gets Tough: Exploring Agent-based Models of Human Performance under Demanding Conditions*
8. Gerben de Vries (UvA) *Kernel Methods for Vessel Trajectories*
9. Ricardo Neisse (UT) *Trust and Privacy Management Support for Context-Aware Service Platforms*
10. David Smits (TU/e) *Towards a Generic Distributed Adaptive Hypermedia Environment*
11. J.C.B. Rantham Prabhakara (TU/e) *Process Mining in the Large: Preprocessing, Discovery, and Diagnostics*
12. Kees van der Sluijs (TU/e) *Model Driven Design and Data Integration in Semantic Web Information Systems*
13. Suleman Shahid (UvT) *Fun and Face: Exploring non-verbal expressions of emotion during playful interactions*
14. Evgeny Knutov (TU/e) *Generic Adaptation Framework for Unifying Adaptive Web-based Systems*
15. Natalie van der Wal (VU) *Social Agents. Agent-Based Modelling of Integrated Internal and Social Dynamics of Cognitive and Affective Processes.*
16. Fiemke Both (VU) *Helping people by understanding them – Ambient Agents supporting task execution and depression treatment*

17. Amal Elgammal (UvT) *Towards a Comprehensive Framework for Business Process Compliance*
18. Eltjo Poort (VU) *Improving Solution Architecting Practices*
19. Helen Schonenberg (TU/e) *What's Next? Operational Support for Business Process Execution*
20. Ali Bahramisharif (RUN) *Covert Visual Spatial Attention, a Robust Paradigm for Brain-Computer Interfacing*
21. Roberto Cornacchia (TUD) *Querying Sparse Matrices for Information Retrieval*
22. Thijs Vis (UvT) *Intelligence, politie en veiligheidsdienst: verenigbare grootheden?*
23. Christian Muehl (UT) *Toward Affective Brain-Computer Interfaces: Exploring the Neurophysiology of Affect during Human Media Interaction*
24. Laurens van der Werff (UT) *Evaluation of Noisy Transcripts for Spoken Document Retrieval*
25. Silja Eckartz (UT) *Managing the Business Case Development in Inter-Organizational IT Projects: A Methodology and its Application*
26. Emile de Maat (UvA) *Making Sense of Legal Text*
27. Hayrettin Gürkök (UT) *Mind the Sheep! User Experience Evaluation & Brain-Computer Interface Games*
28. Nancy Pascall (UvT) *Engendering Technology Empowering Women*
29. Almer Tigelaar (UT) *Peer-to-Peer Information Retrieval*
30. Alina Pommeranz (TUD) *Designing Human-Centered Systems for Reflective Decision Making*
31. Emily Bagarukayo (RUN) *A Learning by Construction Approach for Higher Order Cognitive Skills Improvement, Building Capacity and Infrastructure*
32. Wietske Visser (TUD) *Qualitative multi-criteria preference representation and reasoning*
33. Rory Sie (OU) *Coalitions in Cooperation Networks (COCOON)*
34. Pavol Jancura (RUN) *Evolutionary analysis in PPI networks and applications*
35. Evert Haasdijk (VU) *Never Too Old To Learn – On-line Evolution of Controllers in Swarm-and Modular Robotics*
36. Denis Ssebugwawo (RUN) *Analysis and Evaluation of Collaborative Modeling Processes*
37. Agnes Nakakawa (RUN) *A Collaboration Process for Enterprise Architecture Creation*
38. Selmar Smit (VU) *Parameter Tuning and Scientific Testing in Evolutionary Algorithms*
39. Hassan Fatemi (UT) *Risk-aware design of value and coordination networks*
40. Agus Gunawan (UvT) *Information Access for SMEs in Indonesia*
41. Sebastian Kelle (OU) Game Design Patterns for Learning
42. Dominique Verpoorten (OU) *Reflection Amplifiers in self-regulated Learning*
43. Withdrawn
44. Anna Tordai (VU) *On Combining Alignment Techniques*
45. Benedikt Kratz (UvT) *A Model and Language for Business-aware Transactions*
46. Simon Carter (UVA) *Exploration and Exploitation of Multilingual Data for Statistical Machine Translation*
47. Manos Tsagkias (UVA) *Mining Social Media: Tracking Content and Predicting Behavior*
48. *Jorn Bakker (TUE) Handling Abrupt Changes in Evolving Time-series Data*
49. Michael Kaisers (UM) *Learning against Learning – Evolutionary dynamics of reinforcement learning algorithms in strategic interactions*
50. Steven van Kervel (TUD) *Ontologogy driven Enterprise Information Systems Engineering*
51. Jeroen de Jong (TUD) *Heuristics in Dynamic Scheduling; a practical framework with a case study in elevator dispatching*

2013

1. Viorel Milea (EUR) *News Analytics for Financial Decision Support*
2. Erietta Liarou (CWI) *MonetDB/DataCell: Leveraging the Column-store Database Technology for Efficient and Scalable Stream Processing*
3. Szymon Klarman (VU) *Reasoning with Contexts in Description Logics*
4. Chetan Yadati (TUD) *Coordinating autonomous planning and scheduling*
5. Dulce Pumareja (UT) *Groupware Requirements Evolutions Patterns*
6. Romulo Goncalves (CWI) *The Data Cyclotron: Juggling Data and Queries for a Data Warehouse Audience*
7. Giel van Lankveld (UT) *Quantifying Individual Player Differences*

8. Robbert-Jan Merk (VU) *Making enemies: cognitive modeling for opponent agents in fighter pilot simulators*
9. Fabio Gori (RUN) *Metagenomic Data Analysis: Computational Methods and Applications*
10. Jeewanie Jayasinghe Arachchige (UvT) *A Unified Modeling Framework for Service Design*
11. Evangelos Pournaras (TUD) *Multi-level Reconfigurable Self-organization in Overlay Services*
12. Marian Razavian (VU) *Knowledge-driven Migration to Services*
13. Mohammad Safiri(UT) *Service Tailoring: User-centric creation of integrated IT-based homecare services to support independent living of elderly*
14. Jafar Tanha (UVA) *Ensemble Approaches to Semi-Supervised Learning Learning*
15. Daniel Hennes (UM) Multiagent Learning – Dynamic Games and Applications
16. Eric Kok (UU) *Exploring the practical benefits of argumentation in multi-agent deliberation*
17. Koen Kok (VU) *The PowerMatcher: Smart Coordination for the Smart Electricity Grid*
18. Jeroen Janssens (UvT) *Outlier Selection and One-Class Classification*
19. Renze Steenhuizen (TUD) *Coordinated Multi-Agent Planning and Scheduling*
20. Katja Hofmann (UvA) *Fast and Reliable Online Learning to Rank for Information Retrieval*
21. Sander Wubben (UvT) *Text-to-text generation by monolingual machine translation*
22. Tom Claassen (RUN) *Causal Discovery and Logic*
23. Patricio de Alencar Silva (UvT) *Value Activity Monitoring*
24. Haitham Bou Ammar (UM) *Automated Transfer in Reinforcement Learning*
25. Agnieszka Anna Latoszek-Berendsen (UM) *Intention-based Decision Support. A new way of representing and implementing clinical guidelines in a Decision Support System*
26. Alireza Zarghami (UT) *Architectural Support for Dynamic Homecare Service Provisioning*
27. Mohammad Huq (UT) *Inference-based Framework Managing Data Provenance*
28. Frans van der Sluis (UT) *When Complexity becomes Interesting: An Inquiry into the Information eXperience*
29. Iwan de Kok (UT) *Listening Heads*
30. Joyce Nakatumba (TUE) *Resource-Aware Business Process Management: Analysis and Support*
31. Dinh Khoa Nguyen (UvT) *Blueprint Model and Language for Engineering Cloud Applications*
32. Kamakshi Rajagopal (OUN) *Networking For Learning; The role of Networking in a Lifelong Learner's Professional Development*
33. Qi Gao (TUD) *User Modeling and Personalization in the Microblogging Sphere*
34. Kien Tjin-Kam-Jet (UT) *Distributed Deep Web Search*
35. Abdallah El Ali (UvA) *Minimal Mobile Human Computer*
36. Than Lam Hoang (TUe) *Pattern Mining in Data Streams*
37. Dirk Börner (OUN) *Ambient Learning Displays*
38. Eelco den Heijer (VU) *Autonomous Evolutionary Art*
39. Joop de Jong (TUD) *A Method for Enterprise Ontology based Design of Enterprise Information Systems*
40. Pim Nijssen (UM) *Monte-Carlo Tree Search for Multi-Player Games*
41. Jochem Liem (UVA) *Supporting the Conceptual Modelling of Dynamic Systems: A Knowledge Engineering Perspective on Qualitative Reasoning*
42. Léon Planken (TUD) *Algorithms for Simple Temporal Reasoning*
43. Marc Bron (UVA) *Exploration and Contextualization through Interaction and Concepts*

2014

1. Nicola Barile (UU) *Studies in Learning Monotone Models from Data*
2. Fiona Tuliyano (RUN) *Combining System Dynamics with a Domain Modeling Method*
3. Sergio Raul Duarte Torres (UT) *Information Retrieval for Children: Search Behavior and Solutions*
4. Hanna Jochmann-Mannak (UT) *Websites for children: search strategies and interface design – Three studies on children's search performance and evaluation*
5. Jurriaan van Reijsen (UU) *Knowledge Perspectives on Advancing Dynamic Capability*
6. Damian Tamburri (VU) *Supporting Networked Software Development*
7. Arya Adriansyah (TUE) *Aligning Observed and Modeled Behavior*
8. Samur Araujo (TUD) *Data Integration over Distributed and Heterogeneous Data Endpoints*
9. Philip Jackson (UvT) *Toward Human-Level Artificial Intelligence: Representation and Computation of Meaning in Natural Language*

10. Ivan Salvador Razo Zapata (VU) *Service Value Networks*
11. Janneke van der Zwaan (TUD) *An Empathic Virtual Buddy for Social Support*
12. Willem van Willigen (VU) *Look Ma, No Hands: Aspects of Autonomous Vehicle Control*
13. Arlette van Wissen (VU) *Agent-Based Support for Behavior Change: Models and Applications in Health and Safety Domains*
14. Yangyang Shi (TUD) *Language Models With Meta-information*
15. Natalya Mogles (VU) *Agent-Based Analysis and Support of Human Functioning in Complex Socio-Technical Systems: Applications in Safety and Healthcare*
16. Krystyna Milian (VU) *Supporting Trial Recruitment and Design by Automatically Interpreting Eligibility Criteria*
17. Kathrin Dentler (VU) *Computing Healthcare Quality Indicators Automatically: Secondary Use of Patient Data and Semantic Interoperability*
18. Mattijs Ghijsen (VU) *Methods and Models for the Design and Study of Dynamic Agent Organizations*
19. Vincius Ramos (TUE) *Adaptive Hypermedia Courses: Qualitative and Quantitative Evaluation and Tool Support*
20. Mena Habib (UT) *Named Entity Extraction and Disambiguation for Informal Text: The Missing Link*
21. Kassidy Clark (TUD) *Negotiation and Monitoring in Open Environments*
22. Marieke Peeters (UT) *Personalized Educational Games – Developing Agent-Supported Scenario-based Training*
23. Eleftherios Sidirourgos (UvA/CWI) *Space Efficient Indexes for the Big Data Era*
24. Davide Ceolin (VU) *Trusting Semi-structured Web Data*
25. Martijn Lappenschaar (RUN) *New Network Models for the Analysis of Disease Interaction*
26. Tim Baarslag (TUD) *What to Bid and When to Stop*
27. Rui Jorge Almeida (EUR) *Conditional Density Models Integrating Fuzzy and Probabilistic Representations of Uncertainty*
28. Anna Chmielowiec (VU) *Decentralized k-Clique Matching*
29. Jaap Kabbedijk (UU) *Variability in Multi-Tenant Enterprise Software*
30. Peter de Kock (UvT) *Anticipating Criminal Behaviour*
31. Leo van Moergestel (UU) *Agent Technology in Agile Multiparallel Manufacturing and Product Support*
32. Naser Ayat (UVA) *On Entity Resolution in Probabilistic Data*
33. Tesfa Tegegne Asfaw (RUN) *Service Discovery in eHealth*
34. Christina Manteli (VU) *The Effect of Governance in Global Software Development: Analyzing Transactive Memory Systems*
35. Joost van Oijen (UU) *Cognitive Agents in Virtual Worlds: A Middleware Design Approach*
36. Joos Buijs (TUE) *Flexible Evolutionary Algorithms for Mining Structured Process Models*
37. Maral Dadvar (UT) *Experts and Machines United Against Cyberbullying*
38. Danny Plass-Oude Bos (UT) *Making Brain-computer Interfaces Better: Improving Usability Through Post-processing*
39. Jasmina Mariæ (UvT) *Web Communities, Immigration and Social Capital*
40. Walter Omona (RUN) *A Framework for Knowledge Management Using ICT in Higher Education*
41. Frederic Hogenboom (EUR) *Automated Detection of Financial Events in News Text*
42. Carsten Eijckhof (CWI/TUD) *Contextual Multidimensional Relevance Models*
43. Kevin Vlaanderen (UU) *Supporting Process Improvement using Method Increments*
44. Paulien Meesters (UvT) *Intelligent Blauw. Met als ondertitel: Intelligence-gestuurde politiezorg in gebiedsgebonden eenheden*
45. Birgit Schmitz (OUN) *Mobile Games for Learning: A Pattern-Based Approach*
46. Ke Tao (TUD) *Social Web Data Analytics: Relevance, Redundancy, Diversity*
47. Shangsong Liang (UVA) *Fusion and Diversification in Information Retrieval*

2015

1. Niels Netten (UvA) *Machine Learning for Relevance of Information in Crisis Response*
2. Faiza Bukhsh (UvT) *Smart auditing: Innovative Compliance Checking in Customs Controls*
3. Twan van Laarhoven (RUN) *Machine learning for network data*
4. Howard Spoelstra (OUN) *Collaborations in Open Learning Environments*
5. Christoph Bösch (UT) *Cryptographically Enforced Search Pattern Hiding*

6. Farideh Heidari (TUD) *Business Process Quality Computation – Computing Non-Functional Requirements to Improve Business Processes*
7. Maria-Hendrike Peetz (UvA) *Time-Aware Online Reputation Analysis*
8. Jie Jiang (TUD) *Organizational Compliance: An agent-based model for designing and evaluating organizational interactions*
9. Randy Klaassen (UT) *HCI Perspectives on Behavior Change Support Systems*
10. Henry Hermans (OUN) *OpenU: design of an integrated system to support lifelong learning*
11. Yongming Luo (TUE) *Designing algorithms for big graph datasets: A study of computing bisimulation and joins*
12. Julie M. Birkholz (VU) *Modi Operandi of Social Network Dynamics: The Effect of Context on Scientific Collaboration Networks*
13. Giuseppe Procaccianti (VU) *Energy-Efficient Software*
14. Bart van Straalen (UT) *A cognitive approach to modeling bad news conversations*
15. Klaas Andries de Graaf (VU) *Ontology-based Software Architecture Documentation*
16. Changyun Wei (UT) *Cognitive Coordination for cooperative Multi-Robot Teamwork*
17. André van Cleeff (UT) *Physical and Digital Security Mechanisms: Properties, Combinations and Trade-offs*
18. Holger Pirk (CWI) *Waste Not, Want Not! – Managing Relational Data in Asymmetric Memories*
19. Bernardo Tabuenca (OUN) *Ubiquitous Technology for Lifelong Learners*
20. Loïs Vanhée (UU) *Using Culture and Values to Support Flexible Coordination*
21. Sibren Fetter (OUN) *Using Peer-Support to Expand and Stabilize Online Learning*
22. Zhemin Zhu (UT) *Co-occurrence Rate Networks*
23. Luit Gazendam (VU) *Cataloguer Support in Cultural Heritage*
24. Richard Berendsen (UVA) *Finding People, Papers, and Posts: Vertical Search Algorithms and Evaluation*
25. Steven Woudenberg (UU) *Bayesian Tools for Early Disease Detection*
26. Alexander Hogenboom (EUR) *Sentiment Analysis of Text Guided by Semantics and Structure*
27. Sándor Héman (CWI) *Updating compressed colomn stores*
28. Janet Bagorogoza (UvT) *Knowledge Management and High Performance; The Uganda Financial Institutions Model for HPO*
29. Hendrik Baier (UM) *Monte-Carlo Tree Search Enhancements for One-Player and Two-Player Domains'*
30. Kiavash Bahreini (OU) *Real-time Multimodal Emotion Recognition in E-Learning*
31. Yakup Koç (TUD) *On the robustness of Power Grids*
32. Jerome Gard (UL) *Corporate Venture Management in SMEs*
33. Frederik Schadd (UM) *Ontology Mapping with Auxiliary Resources*
34. Victor de Graaff (UT) *Gesocial Recommender Systems*
35. Jungxao Xu (TUD) *Affective Body Language of Humanoid Robots: Perception and Effects in Human Robot Interaction*

2016

1. Syed Saiden Abbas (RUN) *Recognition of Shapes by Humans and Machines*
2. Michiel Christiaan Meulendijk (UU) *Optimizing medication reviews through decision support: prescribing a better pill to swallow*
3. Maya Sappelli (RUN) *Knowledge Work in Context: User Centered Knowledge Worker Support*
4. Laurens Rietveld (VU) *Publishing and Consuming Linked Data*
5. Evgeny Sherkhonov (UVA) *Expanded Acyclic Queries: Containment and an Application in Explaining Missing Answers*
6. Michel Wilson (TUD) *Robust scheduling in an uncertain environment*
7. Jeroen de Man (VU) *Measuring and modeling negative emotions for virtual training*
8. Matje van de Camp (TiU) *A Link to the Past: Constructing Historical Social Networks from Unstructured Data*
9. Archana Nottamkandath (VU) *Trusting Crowdsourced Information on Cultural Artefacts*
10. George Karafotias (VUA) *Parameter Control for Evolutionary Algorithms*
11. Anne Schuth (UVA) *Search Engines that Learn from Their Users*
12. Max Knobbout (UU) *Logics for Modelling and Verifying Normative Multi-Agent Systems*

13. Nana Baah Gyan (VU) *The Web, Speech Technologies and Rural Development in West Africa – An ICT4D Approach*
14. Ravi Khadka (UU) *Revisiting Legacy Software System Modernization*
15. Steffen Michels (RUN) *Hybrid Probabilistic Logics – Theoretical Aspects, Algorithms and Experiments*
16. Guangliang Li (UVA) *Socially Intelligent Autonomous Agents that Learn from Human Reward*
17. Berend Weel (VU) *Towards Embodied Evolution of Robot Organisms*
18. Albert Meroño Peñuela (VU) *Refining Statistical Data on the Web*
19. Julia Efremova (Tu/e) *Mining Social Structures from Genealogical Data*
20. Daan Odijk (UVA) *Context & Semantics in News & Web Search*
21. Alejandro Moreno Célleri (UT) *From Traditional to Interactive Playspaces: Automatic Analysis of Player Behavior in the Interactive Tag Playground*
22. Grace Lewis (VU) *Software Architecture Strategies for Cyber-Foraging Systems*
23. Fei Cai (UVA) *Query Auto Completion in Information Retrieval*
24. Brend Wanders (UT) *Repurposing and Probabilistic Integration of Data; An Iterative and data model independent approach*
25. Julia Kiseleva (TU/e) *Using Contextual Information to Understand Searching and Browsing Behavior*
26. Dilhan Thilakarathne (VU) *In or Out of Control: Exploring Computational Models to Study the Role of Human Awareness and Control in Behavioural Choices, with Applications in Aviation and Energy Management Domains*
27. Wen Li (TUD) *Understanding Geo-spatial Information on Social Media*
28. Mingxin Zhang (TUD) *Large-scale Agent-based Social Simulation – A study on epidemic prediction and control*
29. Nicolas Höning (TUD) *Peak reduction in decentralised electricity systems -Markets and prices for flexible planning*
30. Ruud Mattheij (UvT) *The Eyes Have It*
31. Mohammad Khelghati (UT) *Deep web content monitoring*
32. Eelco Vriezekolk (UT) *Assessing Telecommunication Service Availability Risks for Crisis Organisations*
33. Peter Bloem (UVA) *Single Sample Statistics, exercises in learning from just one example*
34. Dennis Schunselaar (TUE) *Title: Configurable Process Trees: Elicitation, Analysis, and Enactment*
35. Zhaochun Ren (UVA) *Monitoring Social Media: Summarization, Classification and Recommendation*
36. Daphne Karreman (UT) *Beyond R2D2: The design of nonverbal interaction behavior optimized for robot-specific morphologies*
37. Giovanni Sileno (UvA) *Aligning Law and Action – a conceptual and computational inquiry*
38. Andrea Minuto (UT) *MATERIALS THAT MATTER – Smart Materials meet Art & Interaction Design*
39. Merijn Bruijnes (UT) *Believable Suspect Agents; Response and Interpersonal Style Selection for an Artificial Suspect*
40. Christian Detweiler (TUD) *Accounting for Values in Design*
41. Thomas King (TUD) *Governing Governance: A Formal Framework for Analysing Institutional Design and Enactment Governance*
42. Spyros Martzoukos (UVA) *Combinatorial and Compositional Aspects of Bilingual Aligned Corpora*
43. Saskia Koldijk (RUN) *Context-Aware Support for Stress Self-Management: From Theory to Practice*
44. Thibault Sellam (UVA) *Automatic Assistants for Database Exploration*
45. Bram van de Laar (UT) *Experiencing Brain-Computer Interface Control*
46. Jorge Gallego Perez (UT) *Robots to Make you Happy*

In the range of books published by the Meijers Research Institute and Graduate School of Leiden Law School, Leiden University, the following titles were published in 2015 and 2016:

MI-247 N. Tezcan, *Legal constraints on EU member states as primary law makers. A Case Study of the Proposed Permanent Safeguard Clause on Free Movement of Persons in the EU Negotiating Framework for Turkey's Accession*, (diss. Leiden), Zutphen: Wöhrmann 2015, ISBN 978 94 6203 828 8

MI-248 S. Thewissen, *Growing apart. The comparative political economy of income inequality and social policy development in affluent countries*, (diss. Leiden), Enschede: Gildeprint 2015, ISBN 978 94 6233 031 3

MI-249 W.H. van Boom, *'Door meten tot weten'. Over rechtswetenschap als kruispunt*, (oratie Leiden), Den Haag: BJu 2015, ISBN 978 94 6290 132 2

MI-250 G.G.B. Boelens, *Het legaat, de wisselwerking tussen civiel en fiscaal recht* (diss. Leiden), 's Hertogenbosch: BoxPress 2015, ISBN 978 94 6295 285 0

MI-251 S.C. Huis, *Islamic Courts and Women's Divorce Rights in Indonesia. The Cases of Cianjur and Bulukumba*, (diss. Leiden), Zutphen: Wöhrmann 2015, ISBN 978 94 6203 865 3

MI-252 A.E.M. Leijten, *Core Rights and the Protection of Socio-Economic Interests by the European Court of Human Rights*, (diss. Leiden), Zutphen: Wöhrmann 2015, ISBN 978 94 6203 864 6

MI-253 O.A. Haazen, *Between a Right and a Wrong. Ordinary Cases, Civil Procedure, and Democracy*, (oratie Leiden), Amsterdam: Amsterdam University Press 2015, ISBN 978 90 8555 099 0

MI-254 A. Marrone, *The Governance of Complementary Global Regimes and the Pursuit of Human Security. The inter-action between the United Nations and the International Criminal Court*, (diss. Leiden), Zutphen: Wöhrmann 2015

MI-255 Marieke Dubelaar, Rick van Leusden, Jeroen ten Voorde, Sigrid van Wingerden, *Alleen voor de vorm? Frequentie, organisatie en praktijk van pro-formazittingen*, Den Haag: Boom Juridische uitgevers 2015, ISBN 978 94 6290 156 8

MI-256 Y. Li, *Inter-creditor Equity in Sovereign Debt Restructuring. Towards the Establishment of a Multilateral Legal Framework* (diss. Leiden), Amsterdam: Amsterdam University Press 2015, ISBN 978 90 8555 103 4

MI-257 M.A.K. Klaassen, *The right to family unification. Between migration control and human rights* (diss. Leiden), Zutphen: Wöhrmann 2015, ISBN 978 94 6203 945 2

MI-258 J.C.W. Gooren, *Een overheid op drift* (diss. Leiden), Zutphen: Wöhrmann 2015, ISBN 978 94 6203 973 5

MI-259 S. Tjandra, *Labour Law and Development in Indonesia* (diss. Leiden), Zutphen: Wöhrmann 2016, ISBN 978 94 6203 981 0

MI-260 R.H.C. van Kleef, *Liability of football clubs for supporters' misconduct. A study into the interaction between disciplinary regulations of sports organisations and civil law* (diss. Leiden), Den Haag: Eleven International Publishing (BJu) 2016, ISBN 978 94 6236 670 1

MI-261 C.G. Breedveld-de Voogd, A.G. Castermans, M.W. Knigge, T. van der Linden & H.A. ten Oever (red.), *Core Concepts in the Dutch Civil Code. Continuously in Motion*, BWKJ nr. 30, Deventer: Kluwer 2016, ISBN 978 90 1313 725 5

MI-262 P.W. den Hollander, *De relativiteit van wettelijke normen*, (diss. Leiden)

MI-263 W. Wels, *Dead body management in armed conflict: paradoxes in trying to do justice to the dead*, (Jongbloed scriptieprijs 2015), Den Haag: Jongbloed 2015, ISBN 979 70 9003 825 9

MI-264 Fredericks, E.A., *Contractual Capacity in Private International Law*, (diss. Leiden), Zutphen: Wöhrmann 2016

MI-265 J.H. Crijns, B.J.G. Leeuw & H.T. Wermink, *Pre-trial detention in the Netherlands: legal principles versus practical reality*, Research Report, Den Haag: Eleven International Publishing (BJu) 2016, ISBN 978 94 6236 687 9

MI-266 B.E.E.M. Cooreman, *Addressing global environmental concerns through trade measures: Extraterritoriality under WTO law from a comparative perspective*, (diss. Leiden), Zutphen: Wöhrmann 2016

MI-267 J.E. van de Bunt, *Het rampenfonds*, (diss. Leiden), Meppel: PrintSupport4U, 2016.

MI-268 J.G.H. Altena, *Het legaliteitsbeginsel en de doorwerking van Europees recht in het Nederlandse materiële strafrecht*, (diss. Leiden), Deventer: Kluwer 2016, ISBN 978 90 1313 885 6

MI-269 D. van der Blom, *De verhouding van staat en religie in een veranderende Nederlandse samenleving*, (diss. Leiden), Zutphen: Wöhrmann 2016, ISBN 978 94 6328 032 7

MI-270 J.M. Hartmann, *A blessing in disguise?! Discretion in the context of EU decision-making, national transportation and legitimacy regarding EU directives*, (diss. Leiden), Amsterdam University Press 2016

MI 271 J.M.J. van Rijn van Alkemade, *Effectieve rechtsbescherming bij de verdeling van schaarse publieke rechten*, (diss. Leiden), Den Haag: Eleven International Publishing (BJu) 2016, ISBN 978 94 6290 301 2, ESBN 978 94 6274 623 7

MI-272 J. Wang, *Trends in social assistance, minimum income benefits and income polarization in an international perspective*, (diss. Leiden), Enschede: Gildeprint 2016, ISBN 978 94 6233 373 4

MI-273 A.J. Metselaar, *Drie rechters en één norm. Handhaving van de Europese staatssteunregels voor de Nederlandse rechter en de grenzen van de nationale procedurele autonomie*, Deventer: Wolters Kluwer 2016, ISBN 978 90 1313 988 4

MI-274 E.J.M. Vergeer, *Regeldruk vanuit een ander perspectief. Onderzoek naar de beleving van deregulering bij ondernemers*, (diss. Leiden)

For the complete list of titles (in Dutch), see: www.law.leidenuniv.nl/onderzoek/publiceren

TL;DR: We use a 20th century legal framework as a basis to apply digital investigative methods in cybercrime investigations. This creates interpretation problems and ambiguity for all actors involved in the criminal justice system. The Dutch legal framework must be updated to provide clarity about the regulations that apply to digital investigative methods and adequately protect the individuals involved. This study provides recommendations to update both the Dutch legal framework and the international legal framework.