Universiteit
Leiden
The Netherlands

Investigating cybercrime

Oerlemans, J.J.

Citation
Oerlemans, J. J. (2017, January 10). *Investigating cybercrime*. *Meijers-reeks*. Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University, Leiden. Retrieved from https://hdl.handle.net/1887/44879

Version:	Not Applicable (or Unknown)
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/44879

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle https://openaccess.leidenuniv.nl/handle/1887/44879 holds various files of this Leiden University dissertation

Author: Oerlemans, Jan-Jaap
Title: Investigating cybercrime
Issue Date: 2017-01-10

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.

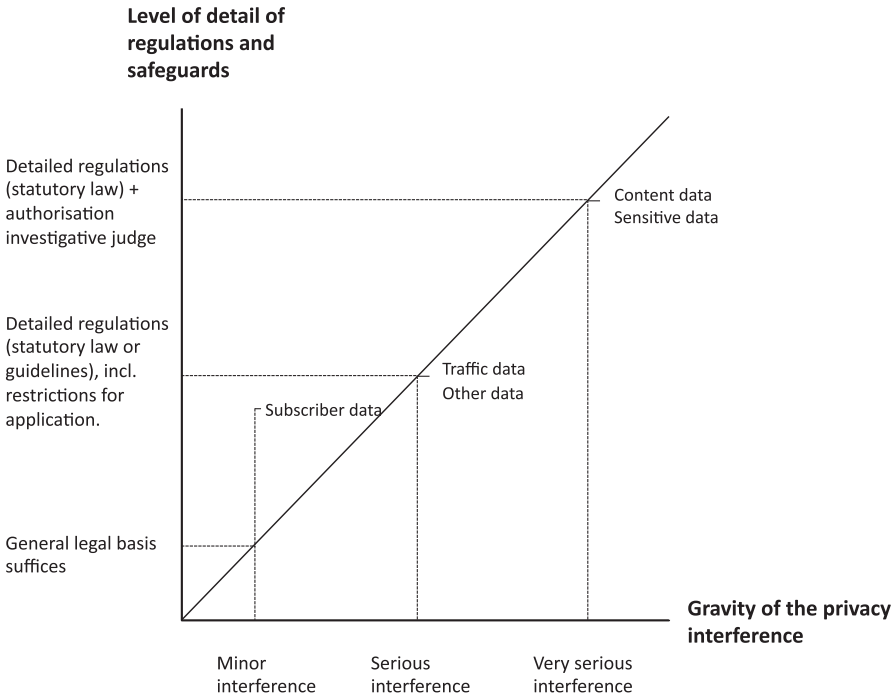

Figure 6.1: Scale of gravity and accompanying quality of the law for data production orders in Dutch criminal procedural law.

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.

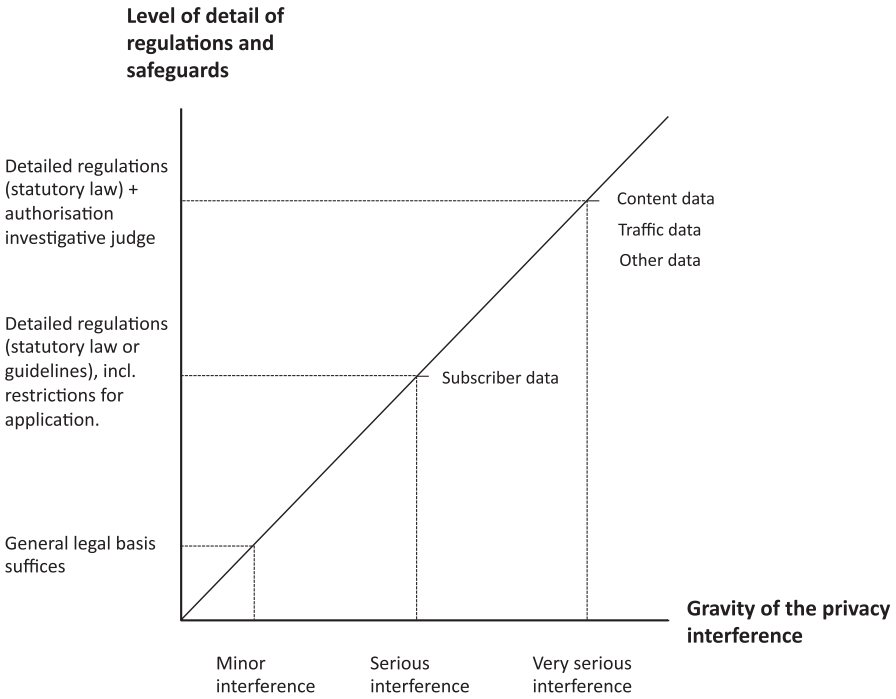

Figure 6.2: The scale of gravity for privacy interferences regarding data production orders that are issued to online service providers and the accompanying desired quality of the law.

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.