Investigating cybercrime

Oerlemans, J.J.

11 Conclusion

This chapter aims to answer the problem statement by answering the four research questions that guided this study. The problem statement (PS) is formulated as follows.

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

The chapter is structured as follows. In section 11.1, the first research question (RQ 1) is answered by explaining which investigative methods are commonly used in cybercrime investigations. In section 11.2, the results of the analysis of the right to privacy in relation to the identified investigative methods are presented. The second research question (RQ 2) is then answered by identifying the normative requirements for the regulation of investigative methods. This section also answers the third research question (RQ 3) by determining which quality of the law is desirable for the identified investigative methods. In section 11.3, the fourth research question (RQ 4) is answered through an overview of the results of the analysis of the Dutch legal framework with regard to the identified digital investigative methods (which is based on the three normative requirements extracted from art. 8 ECHR). The overview also incorporates the recommendations to adequately regulate the identified digital investigative methods in Dutch criminal procedural law. In section 11.4, the fifth research question (RQ 5) is answered by suggesting restrictions to the cross-border unilateral application of the identified digital investigative methods. The answers to these five research questions should provide the knowledge necessary to answer the problem statement (PS) in section 11.5. Finally, section 11.6 provides recommendations that are based on the results of this study.

11.1 Digital investigative methods

The first research question was formulated as follows.

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

The analysis in chapter 2 has shown that law enforcement officials often follow two digital leads, namely IP addresses and online handles, to gather evidence in cybercrime investigations. These digital leads can help them to identify an individual and prove that person committed a cybercrime. How-

ever, cybercriminal investigations are seldom straightforward, due to the following three challenges that often arise: (1) anonymity, (2) encryption, and (3) jurisdiction.

Despite these challenges, law enforcement officials can use novel investigative methods to find the initial digital leads and following-up on them to gather evidence in criminal investigations with regard to cybercrime. An analysis of the investigative activities of law enforcement officials in cybercrime investigations revealed that the following investigative methods are commonly used in cybercrime investigations:

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

In cybercrime investigations, law enforcement officials can gather evidence *unilaterally across State borders*. Law enforcement officials will remain in the territory of the investigating State to gather evidence, yet produce extraterritorial effects through their use of their investigative methods. The investigative methods can also be applied unilaterally, which means that no permission is obtained to gather evidence on the territory of the affected State and no authorising legal basis in a treaty is available for the evidence-gathering activity. This application of investigative methods gives rise to questions related to international law, which are addressed by RQ 5 (see section 11.4).

11.2 The right to privacy and digital investigative methods

The second research question was formulated as follows.

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

In chapter 3, the right to privacy as articulated in art. 8 ECHR was further examined to determine the normative requirements for the regulation of investigative methods. The analysis showed that the scope of protection under art. 8 ECHR is rather broad, which means that the application of many investigative methods interfere with the right privacy. Investigative methods that interfere with the right to privacy must meet the following three conditions in order to be considered legitimate under art. 8 ECHR: they must (1) have a legitimate aim, (2) be in accordance with the law, and (3) be necessary in a democratic society. In relation to the regulation of investigative methods, the second condition of being '*in accordance with the law*' is most important.

This condition of being 'in accordance with the law' requires that the regulations for investigative methods (1) be accessible, (2) be foreseeable, and (3) meet a certain quality of the law. These are considered to be the nor-

mative requirements for regulating investigative methods. The first normative requirement, namely accessibility, means that the law gives an adequate indication concerning the regulations for the use of investigative methods in a given case. The second normative requirement, foreseeability, implies that the legal framework for investigative methods prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which the investigative method is exercised. The third normative requirement, i.e., the quality of the law, means that regulations concerning investigative methods must be of sufficient quality. The ECtHR can specify the level of detail of the regulations and the minimum procedural safeguards that must be implemented in regulations concerning investigative methods that interfere with the right to privacy in this regard. Depending on the gravity of the privacy interference that takes place, the ECtHR requires more or less detailed law and procedural safeguards for regulating investigative methods. This mechanism, which is referred to as the 'scale of gravity for privacy interferences', was illustrated in Figure 3.1 in chapter 3 and has been important in determining the desired requirements for the regulation of the identified digital investigative methods. The scale of gravity also provided a tool for visualising the privacy interferences and locating them within the Dutch legal framework, which enabled the detection of misalignments between the quality of the law of current Dutch regulations and the desired quality of the law as that flows forth from art. 8 ECHR.

The third research question was formulated as follows.

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

Chapter 4 examined all of the identified digital investigative methods in relation to the right to privacy as articulated in art. 8 ECHR. The application of each investigative method interferes with the right to privacy in a different and specific manner. The ECtHR sets specific requirements for each method, depending on the gravity of the privacy interference that takes place. As the privacy interference becomes more intrusive, the ECtHR requires more detailed regulations and specific procedural safeguards. With regard to undercover investigative methods, the ECtHR has articulated qualitative requirements for the domestic legal frameworks of contracting States to prevent entrapment from occurring and to ensure a fair trial based on art. 6 ECHR. These requirements are such that it is possible to transpose them to requirements for the *regulation* of undercover operations. The identified normative requirements derived from art. 8 ECHR were thus still appropriate for testing the adequacy of the Dutch legal framework for undercover investigative methods.

The ECtHR interprets convention rights, including art. 8 ECHR, according to present-day standards. This is important in respect to digital investigative methods, since they can interfere with the right to privacy in new ways. The analysis in chapter 4 showed that no case law that specifically concerns the relation between art. 8 ECHR and the identified digital investigative method is available. Therefore, the *desirable* requirements for the investigative methods was formulated based on case law regarding similar 'counterpart' investigative methods and an analysis of the gravity of the privacy interference according to present-day standards and conditions. An overview of the desirable quality of the law articulated for each of the investigative methods is provided in Table 4.1 in chapter 4.

11.3 Regulating digital investigative methods

The fourth research question was formulated as follows.

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

In chapters 5 to 8, the Dutch legal framework that regulates the identified digital investigative methods was tested against the normative requirements in art. 8 ECHR. This assessment helped to detect misalignments between the Dutch legal framework and the normative requirements based on art. 8 ECHR. The results of the assessment were then used to formulate recommendations for improvements in relation to all of the identified digital investigative methods. The results of the assessment of the Dutch legal framework based on the normative requirements and an overview of the recommendations is presented below in table 11.1.

Investigative method	**Accessibility**	**Foreseeability**	**Quality of the law**	**Recommendations**
1. *Gathering publicly available online information* A. Manual gathering of publicly available online information B. Automated gathering of publicly available online information C. Observing online behaviours of individuals	A. ✓ B. ✓ C. ✓	A. ✗ B. ✗ C. ✗	A. ✓ B. ✗ C. ✗	(1) Create a guideline for the manual gathering of publicly available online information. (2) Create detailed regulations (in statutory law) for the automated gathering of publicly available online information. (3) Create a guideline for the observation of online behaviours of individuals or amend the special investigative power for systematic observation.
2. *Issuing data production orders to online service providers* A. Subscriber data B. Traffic data C. Other data D. Content data	A. ✓ B. ✓ C. ✓ D. ✓	A. ✗ B. ✗ C. ✗ D. ✗	A. ✓ B. ✗ C. ✗ D. ✗	(1) Merge the dual regime for data production orders into a single regime. (2) Clearly define each category of data in lower regulations. (3) Introduce a warrant requirement for obtaining traffic and other data.
3. *Applying online undercover investigative methods* A. Online pseudo-purchases B. Online undercover interactions C. Online infiltration operations	A. ✓ B. ✓ C. ✓	A. ✓ B. ✗ C. ✓	A. ✓ B. ✗ C. ✗	(1) Amend the special investigative power for online pseudo-purchases by removing redundant text. (2) Amend the special investigative power for systematic information gathering to better reflect it incorporates undercover interactions as an investigative method. (3) Amend the special investigative powers for systematic information gathering and infiltration by incorporating the mandatory supervision of an investigative judge.
4. *Performing hacking as an investigative method* A. Network searches B. Remote searches C. The use of policeware	A. ✓ B. ✓ C. ✓	A. ✗ B. ✗ C. ✗	A. ✓ B. ✗ C. ✓	(1) Amend the special investigative power for network searches and include with a warrant requirement. (2) Create a new special investigative power for remotely accessing computers as an investigative method, which includes the power to perform remote searches and use policeware. (3) Restrict the scope of this investigative power and create an exhaustive list of functionalities for policeware.

Table 11.1: An overview of the research results of chapters 5, 6, 7, and 8 (✓ = adequate, ✗ = not adequate).

Table 11.1 illustrates that the first normative requirement of accessibility did not prove to be problematic for the Dutch legal framework. This was to be expected, as the strong legality principle in Dutch criminal procedural law ensures that a legal basis for the investigative methods is most often present in law. However, the foreseeability requirement, i.e., that the legal framework for investigative methods prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which the investigative method is exercised, turned out to be more problematic. In addition, Table 11.1 shows that many of the identified digital investigative methods do not meet the desired quality of the law. It is further examined below how (1) the foreseeability of the regulations for investigative methods and (2) the quality of the law for the identified digital investigative methods can be improved.

Improving foreseeability within the regulations for digital investigative methods

The first and most important observation is that digital investigative methods are currently not regulated in a sufficiently foreseeable manner in Dutch law.[1] The description of investigative methods in legislative history often appear outdated, hardly any case law regarding the identified digital investigative methods is available, and public guidelines often do not mention the investigative methods.

This conclusion is worrisome, since the right to privacy – and ultimately the rule of law – aim to protect individuals from the arbitrary application of power by governmental authorities. More clarity should therefore be provided with regard to the scope of the investigative methods and the manner in which Dutch law enforcement officials apply them.

The Dutch legislature and Public Prosecution Service can make the legal framework more foreseeable by creating more detailed regulations for the application of the identified investigative methods. Three avenues exist for doing so. First, insofar as an investigative method can be placed under an existing special investigative power, the Dutch legislature or Public Prosecution Service should clarify which legal basis is specifically appropriate. This approach is desirable for the following investigative methods: the observation of the online behaviours of individuals, data production orders that are issued to online service providers, and online undercover interactions with individuals. Second, insofar as an investigative method is new and (too) distinct from existing methods to be applied on existing bases, and interferes with the rights and freedoms of the individuals involved in an intrusive manner, a new special investigative power should be created. This avenue is recommended for specific types of hacking as an investigative method. Third, insofar as an investigative method is new but does not interfere with the rights and freedoms of the individuals involved in a particularly intrusive manner, detailed regulations outside of criminal procedural law may

1 With the exception of two online undercover investigative methods. See Table 11.1.

suffice. This avenue is recommended for the manual and automated gathering of publicly available online information.

In addition, the suggestion to create a supervisory commission for the Dutch Police was made in chapter 10 (cf. Buruma 2016, p. 1541). That commission could be charged with controlling and evaluating the evidence-gathering activities of Dutch law enforcement authorities. Its findings could then be reported to the Dutch Parliament and published in public reports. This commission could also identify the need for new regulations as that needs arises, from both law enforcement and fundamental rights perspectives.

Improving the quality of the law

The second observation that can be made is that the Dutch legal framework currently does not have sufficient safeguards in place with regard to specific applications of the identified investigative methods. This statement is further argued below in relation to all four methods.

Dutch law enforcement authorities should realise that they cannot have unlimited access to publicly available online information. Data protection regulations restricts the processing of publicly available information that they gather. However, the Dutch legislature or the Public Prosecution Service should create a guideline that restricts the manual gathering of online information more concretely, by specifying how the data protection regulations should be concretely fulfilled. The pre-emptive storage of personal online information is an intrusive investigative method, since information concerning individuals who have nothing to do with criminal investigations is also stored. Furthermore, the collected data can be further processed and enriched in order to gain a more intricate picture of individuals' lives. For that reason, a recommendation was made to create detailed regulations for the automated gathering of publicly available online information. The analysis also showed that the existing safeguards in the Dutch legal framework suffice for the observation of individuals' online behaviours. However, the Dutch legislator or Public Prosecution Service should create a guideline that specifies more explicitly under which conditions this investigative method can be applied and when the application of the investigative method should be considered systematic.

Detailed regulations already exist in Dutch criminal procedural law in relation to data production orders. However, it is not sufficiently clear what kind of data falls into which category (the 'What-question') and which of two regimes for data production orders applies to online service providers (the 'Who-question'). Lower regulations should specify lists of data that fall the categories of data that can be obtained with data production orders, which are regulated as special investigative powers. In addition, more safeguards – such as a warrant from an investigative judge – should be considered for data production orders with regard to traffic and other data that are issued to online service providers. The reason for this additional safeguard is that the gathering of information from the categories of traffic data

and other data are particularly intrusive investigative methods. When this investigative method is being regulated, it should be kept in mind that the collected data can be further analysed with powerful software and enriched with other data. In addition, a warrant requirement should apply for the collection of content data, including stored files that are available at online storage providers.

The Dutch legal framework for the application of undercover investigative methods arguably does not contain sufficient safeguards based on the requirements formulated by the ECtHR in case law in the context of art. 6 ECHR, which can be transposed to art. 8 ECHR requirements. The ECtHR prefers the involvement of an investigative judge to supervise undercover operations. Without such involvement, other 'adequate safeguards' must be available in domestic legal frameworks. It is unclear whether the Dutch legal framework, which only requires that a public prosecutor be involved in the application of (1) pseudo-purchases and -services, (2) systematic information gathering, and (3) infiltration as special investigative powers, currently meets the desired quality of the law. In my view, the involvement of an investigative judge should be mandatory in the regulations for (1) (online) undercover interactions with individuals and (2) (online) infiltration operations. The need for these extra safeguards can be derived from the severe interference with the right to privacy and the dangers to the integrity of criminal investigation that accompany the application of these investigative methods, as well as the high risk of entrapment involved in their application. A risk of entrapment is also present when (online) pseudo-purchases are applied. However, the application of an (online) pseudo-purchase is less privacy intrusive than the other online undercover investigative methods. The special investigative power that regulates the one-time application of (online) pseudo-purchases is therefore is sufficient quality, even though supervision of an investigative judge is not included in the special investigative power.

At the time of writing (October 2016), the Dutch legal framework does not contain sufficient safeguards for the examined applications of hacking as an investigative method. Hacking as an investigative method should be regulated by a special investigative power in the DCCP with a warrant of an investigative judge as a procedural safeguard. A special investigative power is present for a network search, but this special investigative lacks a warrant requirement as a procedural safeguard. The Dutch legislator suggests that a remote search can be applied on the legal basis to search a place in order to secure stored data on computers. However, a remote search does not take place during a search at a place in the physical world and interferes with the right to privacy in a different and more intrusive meaner than regular computer searches, since it is applied remotely and covertly. Therefore a specific provision should be created for remote searches in the DCCP with the procedural safeguard of a warrant of an investigative judge. The use of policeware is the most intrusive digital investigative method that is examined in this study. Policeware can be remotely and covertly installed

on a computer to monitor an individual's computer behaviours. The many functionalities of policeware include the ability (1) to create a backdoor for law enforcement officials to gain remote access to a computer system; (2) to determine the location of the computer and sent back identifying information about that computer to law enforcement authorities; and (3) intercept digital communications at its source and transfer those communications back to law enforcement authorities. The use of policeware requires detailed regulations statutory law and a warrant requirement that restricts the functionalities that are used and the duration that policeware can be used. The special investigative power that authorises the use of policeware meets this quality of the law, but is more limited in scope since it can only be applied insofar the functionalities of software are restricted to recording private communications.

The proposed Computer Crime Act III regulates remote searches and the use of policeware in an only partially adequate manner. The scope of the new investigative power for hacking as an investigative method is particularly broad and should be restricted more clearly in legislation.

11.4 Cross-border unilateral application of digital investigative methods

The fifth research question was formulated as follows.

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

Theoretically speaking, law enforcement officials cannot mount an investigation on foreign territory without permission from the affected State(s) or authority derived from a treaty. However, in practice law enforcement officials use digital investigative methods to collect evidence on foreign territory from their own territory. They thus apply these investigative methods *unilaterally* and *across State borders*. A disparity can currently be identified with regard to the theory of the territorial limitation of enforcement jurisdiction and the cross-border unilateral application of digital investigative methods. States should start including the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. They should also make efforts to agree with other States as to the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable. Chapter 9 examined the extent to which the cross-border unilateral application of the identified investigative methods is acceptable from a Dutch perspective.

The analysis of this research question showed that one consequence of extraterritorial evidence-gathering activities is that the affected State(s) may view the practice as a violation of their territorial sovereignty. How States respond to these interferences depends on the intrusiveness of the inves-

tigative method and factors such as past grievances with other States. In addition, as a corollary of the territorial limitation of enforcement jurisdiction and State sovereignty, the individuals located in a State are protected against arbitrary interferences from *foreign* law enforcement authorities in their private lives. The cross-border unilateral application of investigative methods can therefore lead to a situation in which foreign laws are applied to individuals who are located in the affected State. The foreign regulations that restrict the application of investigative methods are not foreseeable to the individuals involved and endanger legal certainty.

In order to illustrate the different ways in which States view interferences with State sovereignty and the right to privacy when the identified investigative methods are unilaterally applied across State borders, a legal comparison was conducted between the Netherlands and the United States. The analysis ultimately led to the conclusion that cross-border unilateral digital evidence-gathering activities already take place in practice. It was argued that the international community needs to accept the reality that the Internet enables law enforcement officials to engage in cross-border evidence-gathering activities. It would be preferable for the desirable restrictions of these cross-border unilateral evidence-gathering activities to be formulated in multinational treaties. However, a question can be raised as to whether States are willing to restrict evidence-gathering activities, especially since certain digital investigative methods can be covertly applied across State borders. In addition, not all consequences of the cross-border unilateral applications of digital investigative methods are particularly serious in terms of intrusions on sovereignty and dangers to the legal certainty of the individuals involved. However, States must take political repercussions and the reciprocal effects of their extraterritorial digital evidence-gathering practices into account. For that reason, States must formulate their own policies for cross-border unilateral digital evidence-gathering activities while waiting for appropriate multinational treaties to be concluded. Table 9.1 in chapter 9 provides an overview of the restrictions that I believe are desirable for Dutch law enforcement authorities. The debate regarding the cross-border unilateral application of digital investigative methods will hopefully be continued in the future, with States eventually negotiating international treaties that include restrictions that protect both State sovereignty and the fundamental rights and legal certainty of the individuals involved in cybercrime investigations.

11.5 Answering the problem statement

The problem statement (PS) of this study was formulated as follows.

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

In the Netherlands, investigative methods that are used in criminal investigations are regulated in criminal procedural law. As the point of departure in the Special Investigative Powers Act, only those investigative methods that (1) interfere with the involved individuals' right to rights and freedoms in more than a minor way or (2) endanger the integrity of criminal investigations are regulated in detail. As a general principle, the Dutch legislature has stated that the regulations for investigative methods apply both 'offline' and 'online'.

However, this study has shown that a considerable degree of ambiguity exists with regard to (the interpretation of) the regulations for investigative methods in an online context. The detailed regulations for special investigative methods, which often form the counterparts for digital investigative methods and accompanying explanatory memoranda were originally written for application of the methods in the physical world. At the time when the bulk of the regulations for special investigative methods were implemented in Dutch criminal procedural law, i.e., in 1999, the Dutch legislature could also not have foreseen the implications that computers and the Internet would have for the evidence gathering activities by law enforcement officials. The Dutch legislator updated the Dutch legal framework to enable these authorities to gather evidence using data production orders and to combat cybercrime more effectively with the Computer Crime Act II. Despite these legislative efforts, ambiguity remains with regard to scope of all of the identified digital investigative methods and the manner in which they are applied. Hardly any case law is available concerning the application of digital investigative methods. In order words, the Dutch legal framework is not sufficiently foreseeable with regard to digital investigative methods. In addition, the analysis has shown that not all regulations for digital investigative methods meet the desirable quality of the law and have an adequate basis for their cross-border unilateral application.

Therefore, Dutch criminal procedural currently does not adequately regulate investigative methods that are used in cross-border unilateral cybercrime investigations. In this study, suggestions have been made to improve the foreseeability and the quality of the law for the following digital investigative methods: (1) gathering publicly available online information, (2) issuing data production orders to online service providers, (3) applying online undercover investigative methods, and (4) performing hacking as an investigative method. These suggestions are based on the normative requirements that were derived from art. 8 ECHR.

This study has also shown that amending the Dutch legal framework with regard to criminal procedural law will not be enough to adequately regulate digital investigative methods. Dutch criminal procedural law alone cannot sufficiently regulate the investigative methods that are used in cross-border unilateral cybercrime investigations, given that the *international dimension* of digital evidence-gathering activities must be taken into consideration. Amendments to the international legal framework are required. However, a significant hurdle must first be cleared. Most legal scholars who

specialise in international co-operation in criminal justice matters currently fail to see that investigative methods can be applied unilaterally across State borders in an online context. Furthermore, the current legal framework that regulates the extraterritorial evidence-gathering activities of law enforcement officials seems to assume that these officials must still physically cross a State border to gather evidence. The Internet allows for a cross-border application of investigative methods and does not take into consideration the borders of a territorially divided legal world.

The first step is thus to accept that the cross-border unilateral application of digital investigative methods is currently occurring. The second step is to amend the legal framework to allow for the cross-border application of digital investigative methods *to a certain extent*. The amended legal framework should take into account the (1) sovereignty interests of States and (2) the rights and freedoms of the individuals involved, more specifically their legal certainty. These amendments to the international legal framework will take time. Ultimately, harmonisation of the cross-border unilateral application of digital investigative methods is necessary in order to protect both (1) State interests and (2) the rights and freedoms of the individuals involved. In the meantime, States, including the Netherlands, should develop their own policies and formulate the desirable restrictions for cross-border unilateral digital evidence-gathering activities.

11.6 Recommendations

This study has extensively analysed the Dutch legal framework for the regulation of the identified digital investigative methods. It has also examined the desirable restrictions for the cross-border unilateral application of these investigative methods. The collective results of these assessments provide the basis for the recommendations discussed hereinafter, which are divided into two groups: (1) recommendations at the domestic level and (2) recommendations at the international level.

11.6.1 Recommendations at the domestic level

On a domestic level, the Dutch legislature should have a more pro-active attitude towards regulating digital investigative methods. Technological developments occur at a fast pace and the legal framework should attempt to keep up. The analysis has shown that, currently, the examples in legislative history often appear outdated, hardly any case law regarding the identified digital investigative methods is available, and public guidelines often do not mention the investigative methods. The Dutch legislature, in discussion with law enforcement authorities and the Public Prosecution Service, should provide public guidance on the interpretation of the scope of the identified investigative methods and the manner in which they are executed. When the existing legal framework is insufficient, additional regulations

must be proposed. The specific recommendations based on the normative requirements derived from art. 8 ECHR have already been provided in section 11.3 and summarised in Table 11.1.

11.6.2 Recommendations at the international level

There is currently a mismatch between the theory of the territorial limitation of enforcement jurisdiction and the cross-border unilateral application of digital investigative methods. States should start including the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. They should also make efforts to agree with other States as to the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable. States must also formulate their own policies for cross-border unilateral digital evidence-gathering activities while taking into consideration the undesirable consequences of those activities with regard to both State sovereignty and the fundamental rights and legal certainty of the individuals involved. Table 9.1 in section 9.7 presented desirable restrictions for the identified investigative methods from a Dutch perspective. However, these proposals should be considered only as a first step towards developing a policy for cross-border unilateral cybercrime investigations. The details of the desirable procedures and treaty provisions must be subjected to further scientific study. Of course, international organisations also have an important role to play in this regard.

11.7 Concluding remarks

As a final observation, I would like to note that I have been underwhelmed by the amount of existing research concerned with (1) the regulation of digital investigative methods and (2) the cross-border unilateral application of (digital) investigative methods that produce extraterritorial effects. These two developments present legal scholars with fascinating and urgent questions that are currently not being sufficiently addressed.

In practice, technically skilled individuals are experimenting with technologies and evidence-gathering methodologies that can seriously endanger the rights and freedoms of the individuals involved. However, as many IT lawyers are acutely aware of and have undoubtedly advised many times: what is possible technically is not always possible legally.

I therefore end this study with a call for legal scholars in all pertinent legal fields to learn more about IT and evaluate the implications of technological developments on our society. A basic understanding of new technologies is indeed critical if we are to accommodate these technologies within our legal frameworks in an appropriate manner.