9 Cross-border unilateral investigations

So far, the legitimacy of the identified digital investigative methods has only been examined in the context of *domestic* applications. Chapters 5 to 8 reviewed the Dutch legal framework's (1) accessibility, (2) foreseeability, and (3) quality of the law with regard to these investigative methods. However, the Internet is global by nature and does not respect the territorial borders that legally divide our world. The borderless Internet enables cybercriminals to target victims anywhere on the planet and capitalise on jurisdictional borders by using services in States with the most favourable regulations for criminals.

In brief, the issue here is that the investigation and prosecution of cybercrime take place *locally* and are limited by the physical borders of a State, whereas cybercrimes themselves are often *cross-border* in nature (cf. Brenner & Schwerha IV 2002, p. 395). The territorial limitation of enforcement jurisdiction restricts digital evidence-gathering activities. This principle dictates that, without permission from the affected State or an authorising treaty, extraterritorial evidence-gathering activities cannot be undertaken. As a consequence, jurisdiction is a major challenge in cybercrime investigations.[1]

At the same time, the borderless Internet also enables law enforcement officials to gather evidence on foreign territory in a practical manner. When law enforcement officials do so without using mutual legal assistance requests or gaining permission from the affected State, they are undertaking a *cross-border unilateral* investigation. This application of investigative methods may enable law enforcement officials to overcome the aforementioned jurisdictional challenge. However, it still gives rise to consequences that must be further examined to assess the desirability of both applying digital investigative methods unilaterally across State borders and setting certain restrictions. In this context 'desirability' thus refers to a means for gathering evidence in a swift and practical manner that takes an activity's corresponding negative consequences into account.

This chapter explores the fifth research question with regard to the identified investigative methods that are used in cybercrime investigations (RQ 5): *To what extent is it desirable and legitimate that the identified investigative methods are applied unilaterally across State borders?* Three steps are taken to answer this question.

---

1 See section 2.5. As explained there, this study only focuses on enforcement jurisdiction. The jurisdiction to prescribe (i.e., the capacity to make and apply law) and the jurisdiction to adjudicate (i.e., the ability of national courts and other administrative bodies exercising judicial functions to hear and decide on matters) should be considered as givens.

The first step entails identifying the (legal) consequences of the cross-border unilateral application of the identified digital investigative methods. These consequences help to evaluate how the cross-border unilateral application of the identified methods should be regulated and restricted.

In the second step, a legal comparison between the Netherlands and the United States is conducted to illustrate how each State both thinks about the desirable restrictions for the cross-border unilateral application of digital investigative methods and actually regulates the identified methods.

Based on the results of the first two steps, the third step then determines the extent to which Dutch law enforcement officials can apply the identified digital investigative methods unilaterally across State borders. The aim is to pinpoint which of these methods are particularly problematic in this regard, given their consequences. The analysis identifies which investigative methods require (further) development in the international legal framework.

The structure of this chapter follows the three above-mentioned steps. Section 9.1 identifies and examines two consequences of cross-border unilateral digital investigations. In sections 9.2 to 9.5, legal comparisons between the Netherlands and the United States are conducted with regard to (1) the cross-border unilateral application of the investigative methods and (2) the legal frameworks of all four identified investigative methods.[2] Section 9.6 then determines the extent to which Dutch law enforcement officials can apply the investigative methods unilaterally across State borders. Finally, section 9.7 concludes the chapter by presenting a summary of the findings.

9.1 Consequences of cross-border unilateral investigations

Cross-border unilateral investigations are understood here as criminal investigations in which law enforcement officials physically remain in the investigating State's territory but gather evidence on foreign territory without permission from the affected State or the use of mutual legal assistance. The implications of such investigations are identified and examined in this section.

The cross-border unilateral application of investigative methods has two legal consequences that require analysis, namely (1) the infringement of the territorial sovereignty of States and (2) dangers to the legal certainty of the individuals involved in criminal investigations (in the sense that they may be subjected to the application of laws from a State other than the one in which they are located). These consequences are further analysed in subsections 9.1.1 and 9.1.2. Subsection 9.1.3 then summarises the results of the analysis.

2 This is not an exhaustive legal comparison, but a brief overview to determine which substantial differences may exist. Understanding these differences is important, as they reveal consequences that need to be taken into consideration as undesirable effects of the cross-border unilateral application of digital investigative methods.

9.1.1 Interferences with the territorial sovereignty of States

The principle of the territorial limitation of enforcement power dictates that law enforcement authorities cannot mount an investigation on foreign territory without the permission of the affected State or a basis in a treaty that authorises a particular evidence-gathering activity. As explained in subsection 2.5.1, this principle finds its origin in other principles of international law, such as (1) sovereignty, (2) the equality of States, and (3) non-intervention. The territorial restraint on criminal investigations serves first and foremost to protect the territorial sovereignty of States; it is a State's sovereign right to apply its laws and maintain security within its borders.

Ultimately, international law and the territorial limitation of enforcement power seek to ensure a stable world order (cf. Shaw 2008, p. 213 and Koops & Goodwin 2014, p. 20). Conflicts could arise between States if local law enforcement authorities were allowed to cross State borders and gather evidence on foreign territory under their own domestic laws. For that reason, mutual legal assistance functions as a mechanism that enables law enforcement authorities to collect evidence on the territory of other States. Within a mutual legal assistance treaty, a State can specify the conditions under which evidence is gathered by local law enforcement authorities (or foreign law enforcement officials under the supervision of local law enforcement authorities) upon the request of another State.[3]

Allowing a degree of cross-border unilateral evidence-gathering activities

Digital investigative methods that are commonly used in criminal investigations with regard to cybercrime enable law enforcement authorities to collect evidence across State borders, i.e., from the territory of the investigating State on the territory of another State that is affected by the evidence-gathering activity. The reactions of States to these extraterritorial activities cannot be generalised, as they are determined by the intrusiveness of the evidence-gathering activities and factors such as past grievances with the other State involved.

Gill (2013, p. 224-226 in: Ziolkowlski 2013) observes that States are likely not willing to destabilise world order and engage in armed conflict with other States over extraterritorial activities of law enforcement authorities that do not involve 'coercive' activities. Examples of coercive activities include (1) physical sabotage, (2) assassinations, and (3) abductions of individuals on another State's territory (see Gill 2013, p. 224 in: Ziolkowlski 2013). Gill argues that, for instance, extraterritorial espionage activities within the 'cyber domain' generally do not lead to an infringement of State sovereignty that rises to the level that States will engage in armed conflict

3 See further subsection 2.5.2.

(i.e., war) with each other.[4] I believe it is also unlikely that cross-border unilateral cybercrime investigations will lead to armed conflict between States. Of course, the level of power of a State and balance of power with other States also influence their responses to cross-border unilateral evidence-gathering activities (cf. Stessens 2000, p. 282).

Reactions to unilateral extraterritorial evidence-gathering activities

Nonetheless, a State can – and will – react to unilateral extraterritorial activities of law enforcement authorities that it does not deem permissible. At the very least, States can demand (a) an apology, (b) an acknowledgment of the wrongful act, and (c) a commitment to not continue those activities in the future (see Koops & Goodwin 2014, p. 75). Foreign law enforcement authorities who engage in unauthorised extraterritorial evidence-gathering activities on foreign territory can also be prosecuted under the local criminal laws of the affected State (cf. Doyle 2012, p. 22).[5] Furthermore, States can use economic and political sanctions to show their discontent with the practice. For example, the United States imposed economic sanctions on North Korea for allegedly hacking Sony Pictures Entertainment on U.S. territory.[6]

Moreover, under the reciprocity principle, States that conduct extraterritorial investigative activities can expect other States to conduct extraterritorial investigation activities on their own territory under the same circumstances. States therefore cannot allow their law enforcement officials to undertake cross-border unilateral digital investigations without expecting that law enforcement officials from other States will conduct the same activities under similar circumstances on their own territory (cf. Koops & Goodwin 2014, p. 76). In other words, the cross-border unilateral application of digital investigative methods may also have consequences for the territorial sovereignty of the investigating State itself.

---

4 It is notable that some authors argue that proportionate counterattacks are permitted in the case of economic (cyber)espionage activities. See, e.g., Messerschmidt 2013 and Skinner 2014. See also Steward Baker, Orin Kerr, and Eugene Volokh, 'The Hackback Debate', *Steptoe Cyberblog*, 2 November 2012. Available at: http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ (last visited on 29 July 2015) for an analysis of hacking back as a countermeasure in relation to criminal law in the United States and – by comparison – the report of Bert-Jaap Koops and Ronald Leenes entitled 'Acties tegen botnets door SURFnet en bij SURFnet aangesloten instellingen: strafrechtelijke aspecten' regarding criminal law aspects of counterattacks in the Netherlands. Available at: https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/expert_opinion_botnets_leenes_oktober_2013.pdf (last visited on 29 July 2015). This study does not further examine the desirability of countermeasures, since they are outside the scope of the research question.

5 See, e.g., John Leyden, 'Russians accuse FBI agent of hacking', *The Register*, 16 August 2002. Available at: http://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/ (last visited on 30 July 2015).

6 See the press release of the U.S. Department of Treasury, 'Treasury Imposes Sanctions Against the Government of The Democratic People's Republic of Korea', 2 January 2015. Available at: http://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx (last visited on 3 September 2015).

Special circumstances for extraterritorial evidence-gathering activities
In the context of the cross-border unilateral application of investigative methods on the Internet, special circumstances that make cross-border unilateral application more acceptable may arise. The reason is that in an online context, it is not always practically possible to *locate* the extraterritorial effects of the application of investigative methods. For instance, when individuals utilise the anonymising service Tor, it is practically impossible to determine the originating IP address of the network that is used to access the Internet. International law does not clearly establish how the extraterritorial effects of applying digital investigative methods should be localised and which response is appropriate to extraterritorial online evidence-gathering activities. There may be special circumstances under which certain cross-border unilateral evidence-gathering activities may be deemed acceptable – to a certain degree – by States. In this chapter, these special circumstances are identified and examined in the first subsection in sections 9.2 to 9.5.

9.1.2 Dangers to legal certainty

The principle of the territorial limitation of enforcement jurisdiction first protects the territorial sovereignty of States. However, as a corollary, individuals located within the territory of a State are protected against arbitrary interference from *foreign* law enforcement authorities in their private lives. Mutual legal assistance is the formal mechanism to gather evidence on foreign territory in criminal investigations. As Conings (2014, p. 2) points out, legal assistance mechanisms can protect citizens against interferences from foreign law enforcement officials. Mutual assistance treaties stipulate the conditions under which (usually local) law enforcement officials can gather evidence at the request of an investigating State. These conditions provide the individuals involved with legal certainty and protection to the level and conditions agreed to by the two States. It can thus be argued that State sovereignty also serves to protect citizens from external threats, including interferences with their right to privacy by foreign law enforcement officials under a different legal regime than that of the State where the citizens are located (cf. Conings 2014, p. 2).

However, a consequence of cross-border *unilateral* investigations is that legal assistance treaties are ignored, which gives rise to the question to what extent States must protect their citizens from having their lives interfered with by foreign law enforcement authorities in this manner. As explained in chapter 3, States can be held to compliance of the ECHR even outside their own sovereign territory. It can also be envisaged that a positive obligation can also be derived from the ECHR, which imposes a duty for member States to protect its citizens against interferences on their own territory – through the Internet – by foreign agents acting from other jurisdictions. In the absence of case law – to my knowledge – these latter obligations cannot be currently based on the ECHR. However, they could flow forth from broader rule of law requirements, such as those requiring legal certainty.

Individuals within the territorial borders of a State assume that their rights and freedoms are only infringed upon by *local* law enforcement authorities under the conditions stipulated in local criminal procedural law (cf. Siemerink 2000c, p. 240). People cannot be expected to know the regulations for evidence-gathering activities conducted by *foreign* law enforcement authorities. For example, law enforcement officials in State A may communicate with an individual located in State B using electronic communication services facilitated by the Internet in an online undercover investigation. In such a case, the individual involved is subjected to governmental power that is applied by foreign law enforcement authorities. When foreign law enforcement officials apply their own domestic regulations, these regulations cannot be accessible and foreseeable to the individual involved. These foreign officials' use of enforcement power can thus endanger *legal certainty* – and ultimately the rule of law, because the practice leads to an arbitrary interference of governmental authorities in the private lives of the individuals involved (cf. De Smet 1999, p. 144).

9.1.3 Section conclusion

The analyses in subsections 9.1.1 and 9.1.2 have shown that cross-border unilateral investigations (1) interfere with the territorial sovereignty of the affected State and (2) endanger the legal certainty of the individuals involved.

To determine the severity of the interference with the territorial sovereignty of States when investigative methods are unilaterally applied across State borders, it is necessary to consider the intrusiveness of the investigative methods being utilised. States view the intrusiveness of investigative methods and thereby also gravity of the interference with the territorial sovereignty of a State differently when that investigative method is applied extraterritorially. Sections 9.2 to 9.5 therefore present a legal comparison that is conducted to examine how States perceive the intrusiveness of the extraterritorial application of digital investigate methods in terms of territorial sovereignty and the right to privacy of the individuals involved. The legal comparison is conducted between the Netherlands and the United States.[7] The possible existence of special circumstances that may serve as the basis for States deeming that the cross-border unilateral application of certain investigative methods is more acceptable is also explored.

To determine the dangers to legal certainty caused by cross-border unilateral investigations, it is necessary to examine how the regulations of digital investigative methods differ between States and evaluate the extent to which those differences are a threat to legal certainty. In order to explore the similarities and differences in the regulation of digital investigative methods, sections 9.2 to 9.5 also present a legal comparison of these regulations between the Netherlands and the United States.

7 See subsection 1.4.2 for the underlying reasons why these two States were selected.

9.2 The gathering of publicly available online information

This section examines the consequences of the cross-border unilateral gathering of publicly available online information. In subsection 9.2.1, a legal comparison is conducted of how the Netherlands and the United States view the extent to which the cross-border unilateral application of this investigative method interferes with the territorial sovereignty of States. To examine the dangers to the legal certainty of the individuals involved, subsection 9.2.2 presents a legal comparison of the manner in which the two States regulate the investigative method. A section conclusion is then provided in subsection 9.2.3.

9.2.1 Interferences with territorial sovereignty

When law enforcement authorities gather publicly available online information, they copy information from webservers and other computers all over the world. For that reason, one can argue that this type of information gathering produces extraterritorial effects.

A 'computer-orientated jurisdiction principle' is traditionally used to localise a digital investigative method. This principle focuses on the location of a computer to determine the effects of a digital investigative method (cf. Conings & Oerlemans 2013, p. 27). For example, the location of a computer that is remotely accessed by law enforcement authorities pinpoints where the extraterritorial effects of an investigative method take place.

The gathering of publicly available online information can thus interfere with the territorial sovereignty of the State in which the data is located. As a result, that investigation activity can – theoretically – not be applied given the territorial sovereignty of the affected State, unless (1) permission is obtained from the affected State or (2) a legal basis that authorises the evidence-gathering activity is available in a treaty.

Treaty basis for the evidence-gathering activity

The Convention on Cybercrime, which was ratified in Budapest in 2001, explicitly provides a treaty basis for the cross-border unilateral application of this investigative method. The treaty basis is provided in art. 32(a) of the convention, which reads as follows:

"A party may, without the authorisation of another Party: (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically".

Member States of the Convention on Cybercrime thus agree that cross-border unilateral access to publicly available data – which is technically stored in computers that may be located on foreign territory – is permitted, without

the need for legal assistance to acquire the evidence.[8] In other words, the States that have ratified this convention agree that the evidence-gathering activity does not interfere with their territorial sovereignty (cf. Koops 2013, p. 658). As the Netherlands and the United States have both ratified the Convention on Cybercrime,[9] their respective law enforcement officials can access publicly available information stored in computers on each other's territory.

It may be argued that the cross-border unilateral collection of publicly available online data that is stored in a computer on the foreign territory of a State that has not ratified the convention is not allowed without permission and may violate the territorial sovereignty of the affected State (see Koops 2011, p. 43-44). However, this approach would ignore the fact that the cross-border unilateral gathering of publicly available online information has been tacitly tolerated by States for almost two decades (cf. Seitz 2005, p. 38). To my knowledge, no State has either formally asked other States for permission to access publicly available information on the Internet or formally objected to the practice. Seitz (2005, p. 38) submits that the cross-border unilateral application of this investigative method is allowed under *international customary law*. However, customary international law is only created when States or a group of States behave openly in a certain manner because they understand that such behaviour is permitted under international law (Koops & Goodwin 2014, p. 20). In addition, it is required that other States do not object to the practice. Indeed, States have tacitly tolerated the cross-border unilateral gathering of publicly available online information for almost two decades and no State has formally objected to the practice. In addition, the convention's Ad-hoc Subgroup on Transborder Access and Jurisdiction declared in 2013 that:

"transborder access to publicly available data (Article 32(a)) may be considered accepted international practice and part of international customary law even beyond the Parties to the Budapest Convention".[10]

The Council of Europe understands '*transborder access*' as unilateral access to computer data stored on another State's territory without that State's consent (see TC-Y 2014, p. 6). At the same time however, States may not be aware of the evidence-gathering activity on their territory. For example, if a Dutch citizen is active in dealing drugs on an online black market, law enforcement officials can observe the behaviours of that black market's member as part of their domestic criminal investigation. Since most cybercriminals use nicknames on online forums, it is difficult to know which

8 See the explanatory memorandum Convention on Cybercrime, par 293.

9 The Netherlands ratified the convention on 16 November 2006. The United States ratified it on 29 October 2006. See http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (last visited on 24 March 2016).

10 T-CY 2013, p. 10.

States are experiencing the territorial effects of the evidence-gathering activity. In these cases, it is problematic to object to the practice.

Nevertheless, the interference with the territorial sovereignty of other States that takes place when this investigative method is unilaterally applied across State borders appears to be minor in nature. The Convention on Cybercrimes allows for the evidence-gathering activity and States have tacitly tolerated the cross-border unilateral gathering of publicly available online information for almost two decades. The cross-border unilateral gathering of publicly available online information is therefore considered acceptable in this study.

9.2.2 Dangers to legal certainty

The fact that the cross-border unilateral application of this method is accepted does not mean that legal certainty is not endangered. When law enforcement officials apply domestic laws that regulate their investigative methods and these investigative methods affect the rights and freedoms of an individual located on foreign territory, the regulations relating to these methods are not accessible or foreseeable for the individual involved. As such, his legal certainty is endangered. States regulate the gathering of publicly available online information in different manners, as illustrated in this subsection using a brief comparison of the Dutch and U.S. regulations concerning this investigative method.

The Dutch legal framework for the gathering of publicly available online information has already been examined extensively in chapter 5. A summary of the results of that analysis is provided below under A. A brief analysis of the U.S. (federal) regulations for this investigative method is presented under B. Finally, the most important differences between the two sets of regulations are identified under C, to illustrate how the cross-border unilateral application of this investigative method can endanger the legal certainty of the individuals involved.

A Overview of Dutch regulations

In the Netherlands, both the manual and automated gathering of publicly available online information are currently only restricted by data protection regulations. In chapter 5, it was argued that more detailed regulations and a more foreseeable legal framework are required for both of these investigative methods, as data protection regulations are not tailored to them and do not adequately indicate the scope of the methods or the manner in which they are applied in practice. For the manual gathering of publicly available online information, a Public Prosecution Service guideline may suffice. However, it was argued that detailed regulations in statutory law should be created tor the automated gathering of publicly available online information, given that this investigative method is regarded as more privacy intrusive.

The online observation of individuals is regulated in detail as a special investigative power in the Netherlands, insofar as the investigative method is applied systematically. To create a more foreseeable legal framework for this method, it was recommended that guidelines clarify when online observation becomes systematic and hence when the special investigative power is applicable. In the Netherlands, observation is in itself regarded as an investigative method that interferes with the right to privacy of the individual involved.

B Overview of U.S. regulations

The U.S. Supreme Court has made it clear that certain constitutional rights related to the first ten amendments to the U.S. Constitution (i.e., the Bill of Rights) also apply to the evidence-gathering activities of U.S. law enforcement authorities (LaFave et al. 2009b, p. 2). The Fourth Amendment to the U.S. Constitution, which bars the U.S. government from conducting unreasonable searches and seizures in relation to U.S. citizens, is of particular importance to the investigative methods discussed in this study. It should be emphasised that this amendment only protects certain elements of the right to privacy as detailed in art. 8 ECHR. Unlike the Netherlands, the United States does not have a general constitutional 'right to privacy'.

The Fourth Amendment in relation to the investigative method is examined in B.1. Thereafter, whether (federal[11]) regulations of criminal procedures restrict the investigative method at hand is considered in B.2. The (internal) guidelines of U.S. law enforcement authorities that may restrict the investigative method are examined in B.3 (insofar as they are publicly available).

B.1 Fourth Amendment to the U.S. Constitution

The Fourth Amendment reads as follows:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

A textual approach to the Fourth Amendment suggests that searches and seizures are limited to the seizure of physical objects during a search at a physical place. However, the constitutional protection provided by this amendment is broader. The decision in *Katz v. United States* played an important role in broadening its scope.[12]

11 The analysis in this chapter is restricted to U.S. criminal procedural law on a federal level. U.S. states also have the jurisdiction to regulate investigative methods.

12 U.S. Supreme Court 18 December 1967, *Katz v. United States*, 389 U.S. at 347-351 (1967).

In the landmark case of *Katz v. United States* in 1967, the U.S. Supreme Court decided that a warrantless microphone recording of a telephone conversation conducted within a public phone booth was unconstitutional given that it violated the Fourth Amendment.[13] The U.S. Supreme Court thereby decided that the Fourth Amendment not only protects U.S. citizens against a physical search with regard to tangible objects, but also vis-à-vis *intangible* 'objects'.[14] In this case, the intangible object was the telephone conversation held inside a telephone booth. The *Katz* judgement created the possibility that other (digital) investigative methods also fall within the scope of the Fourth Amendment.

The case of *Katz v. United States* is also important, because the '*reasonable expectation of privacy*' doctrine was developed in its decision. In his concurring opinion, justice Harlan developed the test to determine whether a person has a reasonable expectation of privacy. This test has two requirements: (1) the individual must demonstrate a subjective expectation of privacy in relation to the object and (2) this privacy expectation must be one that (U.S.) society recognises as reasonable.[15] After all, the Fourth Amendment only protects citizens against *unreasonable* searches. In the context of gathering publicly available information on the Internet, the following quote from the *Katz v. United States* case is relevant:

"What a person knowingly exposes to the public, (…) is not a subject of Fourth Amendment protection."[16]

Interpreted in an online context, this means that U.S. citizens do not have a reasonable expectation of privacy when they knowingly disclose information on publicly accessible parts of the Internet. The protection of the Fourth Amendment does not apply in this situation (cf. DoJ Manual 2009, p. 5, Kerr 2010, p. 447 and Brenner 2010, p. 194). The above quote in *Katz v. The United States* is clearly referred to in the 2002 case of *U.S. v. Gines-Perez*, in which the judge stated that it is:

"obvious that a claim to privacy is unavailable to someone who places information on an indisputably public medium such as the Internet, without taking any measures to protect that information."[17]

13 U.S. Supreme Court 18 December 1967, *Katz v. United States*, 389 U.S. at 347-351 (1967).

14 Citing the case of U.S. Supreme Court 6 March 1961, *Silverman v. United States*, 365 U.S. at 511 (1961).

15 U.S. Supreme Court 18 December 1967, *Katz v. United States*, 389 U.S. at 361 (1967) (J. Harlan, concurring). Kerr convincingly argues that – in practice – the 'reasonable expectation of privacy test' only consists of one test: whether an individual's expectation of privacy is one that U.S. society recognises as reasonable (Kerr 2014).

16 U.S. Supreme Court 18 December 1967, *Katz v. United States*, 389 U.S. at 351-352 (1967).

17 The U.S. District Court District of Puerto Rico, *United States v. Gines-Perez*, 214 F. Supp. 2d 205, at 225 (2002).

However, publicly available online information is not necessarily disclosed by the individual himself. As such, one can argue that the reasonable expectation of privacy doctrine does not apply when one's personal information is published by others. Yet, another exception to the Fourth Amendment warrant requirement, called the '*public vantage doctrine*', may apply in that situation. The public vantage doctrine means that U.S. law enforcement officials are "*entitled to see anything that any member of the public could see from a similar series of vantage points*" (Stuntz 1995, p. 1022-1023). The cases of *California v. Ciraolo*[18] and *Florida v. Riley*[19] were influential in developing this doctrine (see Petrashek 2009, p. 1523-1524). In the case of *California v. Ciraolo*, U.S. law enforcement officials investigated a report of marijuana growth in the backyard of an individual. They decided to fly a small airplane over the (fenced-in) backyard of the individual to determine whether marijuana plants were indeed present. The suspect objected to this investigative activity and argued that a warrant was required to conduct this search. The U.S. Supreme Court disagreed and concluded that Fourth Amendment was not violated.[20] In *Florida v. Riley*, U.S. law enforcement officials used a helicopter to observe what was located in a partially covered greenhouse in the backyard of a residence. The suspect contended a warrant was required for the investigative activity. Again, the U.S. Supreme Court disagreed and concluded the Fourth Amendment was not violated (and thus no warrant was required for the aerial observation).[21]

Petrashek (2009, p. 1525) explains how the public vantage doctrine is important in the context of the gathering of publicly available online information. The authors cites several cases in which U.S. courts decided that individuals have no reasonable expectation of privacy in the publishing of information on publicly accessible social media websites, chatrooms, and online discussion forums.[22] The reason that these individuals have no reasonable expectation of privacy is that the online information is accessible by anyone. A U.S. federal guideline for a 'Developing a Policy on the Use of

18 U.S. Supreme Court 19 May 1986, *California v. Ciraolo*, 476 US 207 (1986).
19 U.S. Supreme Court 23 January 1989, *Florida v. Riley*, 488 U.S. 445 (1989).
20 U.S. Supreme Court 19 May 1986, *California v. Ciraolo*, 476 US at 215 (1986).
21 U.S. Supreme Court 23 January 1989, *Florida v. Riley*, 488 U.S. at 451 (1989).
22 Citing the cases of U.S. Court of Appeal of California (5th District), *Moreno v. Sentinel, Inc.*, 2 April 2009, no. F054138 (2009), in which the U.S. court stated *"Here, Cynthia publicized her opinions about Coalinga by posting the Ode on myspace.com, a hugely popular internet site. Cynthia's affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material"*, U.S. Court of Appeals for the Armed Forces, 21 November 1996, *United States v. Maxwell*, no. 95-0751 (1996), in which the U.S. court stated: *"Messages sent to the public at large in the 'chat room' or e-mail that is 'forwarded' from correspondent to correspondent lose any semblance of privacy"*, and U.S. Court of Appeals (6th Circuit), 2 July 2001, *Guest v. Leis*, 255 F.3d 325 (2001), in which the U.S. court decided that U.S. law enforcement officials can assume undercover identifies, access an online discussion forum and download images, because "*users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting*".

Social Media in Intelligence and Investigative Activities' confirms that it is part of 'normal law enforcement activity' (based on the law enforcement purpose) to search a suspect's Facebook page that is publicly accessible (cf. Global Justice Information Sharing Initiative 2013, p. 14).[23] The guideline confirms that the evidence gathering activity does not require a warrant. The guideline suggests that only a 'minimal' authorisation level should be required by law enforcement authorities for the manual gathering of publicly available online information (cf. Global Justice Information Sharing Initiative 2013, p. 14).

B.2 U.S. criminal procedural law

The U.S. Congress also influenced criminal procedure law in the United States by establishing the Federal Rules of Criminal Procedure in Title 18 of the U.S. Code. The U.S. Congress may enact legislation governing both federal and state criminal justice systems. However, it has used this authority only sparingly (see LaFave et al. 2009a, p. 18).[24] No federal criminal procedure regulations address the gathering of publicly available online information.

B.3 Guidelines for U.S. law enforcement authorities

U.S. law enforcement authorities are also bound by (internal) guidelines in their evidence-gathering activities. In the United States, individuals involved in criminal investigations cannot derive rights from these guidelines.[25] As a result, these guidelines have a different status than the regulations and guidelines that were discussed in relation to the legal framework in the Netherlands, where citizens can derive rights from these public guidelines. Furthermore, the policies may vary for each U.S. law enforcement authority, both on a local and federal level. However, these guidelines do provide information about how the investigative methods are restricted in practice. Therefore, the relevant aspects are examined below.

The FBI Domestic Investigations and Operations Guide 2011 provides indications about applicable internal regulations. More specifically, the guideline defines publicly available information as follows*:*

23 The guideline explains on p. 13 that a valid law enforcement purpose means that a law enforcement official can, for example, search for and access an individual's Facebook profile to identify an alleged criminal, but not look for information on a new neighbour.

24 Note that U.S. states are sovereign and can also prescribe laws and enforce that code through the agencies and procedures that it creates (see LaFave et al. 2009b, p. 2). Each of the 50 U.S. states has the authority to create criminal procedural law. In addition to these 50 states, (1) the District of Columbia (no. 51) (i.e., the Washington D.C. area) has the power to prescribe and enforce its own laws and (2) the U.S. Congress (no. 52) has created a criminal justice system of its own to enforce the general criminal code by federal agencies in federal courts (see LaFave et al. 2009b, p. 3).

25 See, e.g., the FBI Domestic Investigations and Operations Guide 2011, part 2-10, section 2.5.

"public information is 'Publicly Available Information' that is:
(A) Published or broadcast for public consumption;
(B) Available on request to the public;
(C) Accessible on-line or other to the public;
(D) Available to the public by subscription or purchase;
(E) Made available at a meeting open to the public;
(F) Obtained by visiting any place or attending an event that is open to the public (e.g., public places); or
(G) Observed, heard, smelled, detected or obtained by any casual observer or member of the public and does not involve unconsented intrusion in private places".[26]

Furthermore, the FBI guideline clarifies that U.S. law enforcement officials can (manually) gather publicly available online information without 'supervisory approval'.[27] Unfortunately, the '*On-Line Investigations*' appendix to the internal guideline of the FBI is regarded as classified and is thus not available for analysis.[28] It therefore remains uncertain whether specific regulations apply to the gathering of publicly available online information by the FBI.[29]

With regard to the automated gathering of publicly available online information, no specifics are provided in the FBI guideline. However, the guideline of the U.S. Georgia Bureau of Investigation Investigative Division developed a specific policy for the use of 'social media monitoring tools' (which is a type of automated data collection system).[30] The provisions in the guideline provide an illustration of how the investigative method may be regulated in the internal guideline of a U.S. law authority. The procedure is as follows. Authorisation of the 'Deputy Director of Investigations' is required to use social media monitoring tools in criminal investigations. The request for authorisation must specify: (1) a description of the social media monitoring tool; (2) its purpose and intended use; (3) the social media websites the tool will access; (4) whether the tool is accessing information in the public domain or information protected by privacy settings; and (5) whether information will be retained by the law enforcement authority and if so, the applicable retention period of such information. If approved, the tool may

26 See FBI Domestic Investigations and Operations Guide 2011, part 18-7, section 18.5.1.1.
27 See 18.5.1.3. The article also states that the rule does not apply when a law enforcement official attends a religious service, even in public.
28 FBI Domestic Investigations and Operations Guide 2011, part L-1.
29 In is noteworthy that in the U.S. federal 'Guideline for Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities' puts special emphasis on articulating a policy to determine the accuracy, validity, and/or authenticity of the information that is obtained from social media sites. The validation is important, since the information is often uploaded by users and a wrong classification may lead to privacy violations or inappropriate actions (see, e.g., Global Justice Information Sharing Initiative 2013, p. 15-16). This is indeed important for the gathering of publicly available online information as an investigative method. However, these regulations do not regard the regulation of the investigative method itself. Therefore, they are not further examined in this study.
30 See appendix I of the Global Justice Information Sharing Initiative 2013, p. 32.

be used for 90 days. After 90 days, a summary of the results of the use of the social media monitoring tool must be provided. It is reiterated here it is important to realise that the existence of this single provision in an internal guideline for a local U.S. law enforcement authority does not mean that all U.S. law enforcement currently use this model guideline; its policies to use automated online data collection systems may vary considerably.

The definition of publicly available information in the guideline for domestic FBI investigations indicates that the *online observation* of the behaviours of individuals is also understood as 'gathering publicly available information'.[31] Therefore, the same regulations apply for the online observation of online behaviours of individuals as for the manual gathering of publicly available online information.

Once the information is gathered and processed by U.S. law enforcement officials, data protection guidelines are applicable for the storage of information in the 'criminal intelligence systems' of U.S. law enforcement authorities (cf. Global Justice Information Sharing Initiative 2013, p. 12). The Criminal Intelligence Systems Operation policy, which is part of the Code of Federal Regulations, is the guiding regulation for the storage of information in a criminal intelligence system in the United States (Carter 2009, p. 149). As the specifics of data protection regulations are not of interest to the research question, they are not further examined.

C Notable differences in approach

Regulations related to the gathering of publicly available information are essentially similar in the Netherlands and the United States. Criminal procedural law does not regulate the (manual and automated) gathering of publicly available online information in detail in either State. Data protection regulations pertain to the investigative method, but they are not applied in a concrete manner – which leaves ambiguity with regard to the scope of the investigative method and the manner in which the investigative method is applied.

In the Netherlands, the investigative method is regarded as an activity that interferes with the right to privacy, albeit not in a particularly serious manner. It was suggested that more detailed regulations be created in statutory law for the automated gathering of publicly available online information. A special investigative power restricts the investigative method of the systematic observation of online behaviours.

In the United States, a general right to privacy does not exist in the U.S. Consitution. The investigative method is not restricted by the Fourth Amendment. As such, the warrant requirement does not apply to the investigative method. Furthermore, this method is not restricted by regulations in federal criminal procedural law. Internal guidelines may or may not restrict the investigative method for U.S. law enforcement authorities. However,

31 See FBI Domestic Investigations and Operations Guide 2011, part 18-7, section 18.5.1.1.

individuals cannot derive any rights from these guidelines. In general, it appears that the investigative method is not regarded as particularly an intrusive investigative method and does not require authorisation. One guideline for a local U.S. law enforcement authority indicates that authorisation of a deputy director is required to make use of automated online data collection systems. The examined guidelines do not distinguish between (1) the manual gathering of publicly available online information and (2) the observation of the individuals' online behaviours; instead, they appear to treat everything as the 'gathering of publicly available information'. This can be explained by the U.S. approach that individuals do not have reasonable expectation of privacy in information that is publicly available to anyone, including by use of observation as an investigative method.

Based on the results of the analysis, it is apparent that accessible and foreseeable regulations for the investigative method do not exist in the United States. The situation is not particularly different in Dutch law. However, an important difference is that in Dutch law, detailed regulations in criminal procedural law apply to the observation of individuals' online behaviours. Namely, a special investigative power that requires authorisation from a public prosecutor is required when the investigative method is applied 'systematically'. In contrast, online observation as an investigative method is not restricted by either a warrant requirement or federal criminal procedure rules in the United States. It appears the investigative method is treated as gathering publicly available information as an investigative method, which requires no special authorisation for law enforcement officials to conduct.

9.2.3 Section conclusion

The analysis in this section has shown that the Convention on Cybercrime provides a treaty basis for the cross-border unilateral gathering of publicly available online information. Both the Netherlands and the United States have ratified the convention and agreed that cross-border unilateral evidence-gathering activities do not infringe their territorial sovereignty. In addition, it is argued that the cross-border unilateral application of the investigative method can be regarded as part of customary law. The interferences with other States' territorial sovereignty when the investigative method is unilaterally applied across State borders also appear to be limited. Therefore, it is not likely that States will object to the practice. As a result, mutual legal assistance is not required to obtain evidence through the cross-border unilateral application of this method.

However, the analysis in subsection 9.2.2 has also shown that the legal certainty of Dutch citizens can be endangered when U.S. law enforcement officials systematically observe their behaviours in an online context. All actors in the criminal justice system should be aware that States regulate this investigative method in different manners and the gathering of publicly available online information (including observation) is not restricted to State borders.

9.3 Data production orders

This section examines the consequences of the cross-border unilateral issuing of data production orders to online service providers. Subsection 9.3.1 explores how the Netherlands and the United States each view the desirable restrictions of the cross-border unilateral application of this investigative method. Section 9.3.2 then compares how both States have regulated the investigative method, in order to identify the regulatory differences that illustrate the dangers to legal certainty. A section conclusion is provided in subsection 9.3.3.

9.3.1 Interferences with territorial sovereignty

States in continental Europe, including the Netherlands, generally regard unilateral data production orders that are issued to companies on foreign territory as a violation of the affected State's territorial sovereignty (cf. Stessens 2000, p. 329, Ryngaert 2008, p. 81 and Gercke 2012, p. 277). To obtain information from online service providers that are located abroad using data production orders, Dutch law enforcement authorities thus require permission of the State in which that company is located or a treaty basis that authorises their evidence-gathering activity.

However, State practice reveals a different picture. The reality is that hundreds of millions of individuals utilise online services that are provided by U.S. companies. A complex ICT infrastructure that makes use of cloud computing techniques in data centres located throughout the world supports these services and enables them to be provided to individuals regardless of where they live. Dutch law enforcement authorities require the cooperation of these companies in order to obtain data using data production orders.

Based on the theoretical framework provided above, Dutch law enforcement authorities need permission from the United States or use mutual legal assistance, each time they send a data production order to a U.S. company. Like any other EU State, the Netherlands can be party to both bilateral treaties with other States and multilateral treaties that are created by the Council of Europe or European Commission. This has led to a situation in which many – and a wide variety of – mutual legal assistance treaties are applicable in the Netherlands.[32] Of these treaties, only the Convention on Cybercrime potentially provides a treaty basis to unilaterally issue data production orders to an online service provider on foreign territory.

32 The texts of these treaties are publicly accessible at: https://verdragenbank.overheid.nl/nl (last visited on 30 September 2015).

Treaty provisions in the Convention on Cybercrime?

Art. 32(b) of the Convention on Cybercrime potentially provides a treaty basis for the unilateral issuance of data production orders to foreign online service providers. It reads as follows:

"A Party may, without the authorisation of another Party: (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

This provision may enable law enforcement officials to issue a (domestic) data production order to a company on foreign territory, which can in turn *voluntarily* comply with it (cf. Walden 2011, p. 8, Koops et al. 2012b, p. 37 and UNODC 2013, p. 219).

However, the provision would then assign *companies* the power to decide whether information should be disclosed to law enforcement authorities, whereas *States* have traditionally decided which investigational activities can take place on their territory (cf. Gercke 2012, p. 277). This is why certain States still view companies' voluntary disclosure of information to foreign law enforcement authorities as a violation of their territorial sovereignty (see Koops et al. 2012b, p. 37).[33] Another difficulty is that national laws can limit the voluntary disclosure of data. Most notably, the voluntary disclosure of data to law enforcement authorities may violate data protection regulations.[34]

In 2014, the Working Group of the Convention on Cybercrime on Transborder Access to Computer Systems provided clarity and explicitly stated in its report that art. 32(b) of the Convention on Cybercrime *does not* provide a legal basis for the cross-border unilateral issuance of data production orders to online service providers (TC-Y 2014, p. 7).[35] This convention thus does not provide a treaty basis for issuing data production orders unilaterally

33 Referring to PC-OC (2009) 05, p. 6 and PC-OC (2008) 01, p. 28).

34 See, e.g., the 'Article 29 Working Party's comments on the issue by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime', letter to the Council of Europe, 5 December 2013, p. 3. Koops and Goodwin (2014, p. 45) also point out that data protection law prescribes that only transfers of personal information is only allowed outside the European Economic Area, insofar as the foreign State has an 'adequate level of data protection'. In that respect, it is noteworthy that the Safe Harbour decision (2000/520/EG) for data transfers from EU Member States to the United States has recently been declared invalid (CJEU 6 October 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner)*. In response, new legislation called 'Privacy Shield' was created to replace the Safe Harbour agreement in 2016.

35 The working group also makes it clear that the terms and conditions of an online service do not constitute explicit consent to disclose information on a voluntarily basis to law enforcement authorities, even if these terms and conditions indicate that data may be shared with criminal justice authorities in cases of abuse (see TC-Y 2014, p. 7).

to online service providers located in foreign territory, who can then disclose information voluntarily, although it does specify that such a practice is not necessarily a violation of international law.[36] Ultimately, the convention does not provide clarity on the matter.

State practice

Even though art. 32b of the Convention on Cybercrime does not formally provide a treaty basis for issuing cross-border unilateral data production orders to online service providers, it appears that in practice, online service providers do *voluntarily* disclose information to law enforcement authorities.[37] For example, based on the company's own policy statement, Microsoft voluntarily discloses information to non-U.S. law enforcement authorities. It states on its website that it allows for the voluntary disclosure of *non-content data* to non-U.S. law enforcement authorities *"in response to a valid legal request"* (…) that is *"validated locally and transmitted to our compliance teams."*[38] These 'valid legal requests' must comply with the local laws of the requesting authority, as authenticated by a local team or law firm in the requesting State.[39]

Microsoft's policy thus indicates that it voluntarily discloses non-content data, i.e. (1) subscriber data, (2) traffic data, and (3) other data, to foreign law enforcement authorities under the local laws of the investigating State after a review by local law firm and Microsoft's compliance team. As a consequence, non-U.S. law enforcement authorities can only obtain content data with a U.S. warrant and mutual legal assistance.[40] Microsoft's transparency reports show that the company has not disclosed any content data to Dutch law enforcement authorities in the past, although it has disclosed subscriber and other data.[41]

The territorial effects of data production orders are traditionally determined by the location of the data that is disclosed to law enforcement authorities. Following this line of reasoning, the State in which data is located dictates the terms concerning how information is disclosed to law

36 See TC-Y 2014, p. 6.

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

38 Available at: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/ (last visited on 30 July 2015). Emphasis added by the author.

39 See http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/ (last visited on 30 July 2015).

40 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 9-10. For a different viewpoint, see Odinot et al. (2013, p. 40) and Koops et al. (2012, p. 20 and p. 38-40), who indicate that Dutch law enforcement authorities reportedly have to use mutual legal assistance procedures to obtain data from U.S. online service providers. It seems to depend on the service provider and the type of information whether information is voluntarily disclosed to law enforcement authorities.

41 Available at: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ (last visited on 30 July 2015).

enforcement authorities (as part of its sovereign rights). Spoenle (2010, p. 4-5) points out that due to cloud computing techniques, the location of data can no longer reasonably determined. Due to cloud computing techniques, data can continuously move between servers. This is called the 'loss of knowledge of location' problem for law enforcement authorities (see Koops & Goodwin 2014, p. 48). When the location of data cannot be ascertained, it is difficult to determine a data production order's extraterritorial effects.

However, taking account the practice of the voluntarily disclosure of data described above, it appears that it is more likely that the location of the online service provider that controls the information determines which regulations apply (cf. UNODC 2013, p. 216). The online service provider can extract the data being sought from its servers in different locations around the world and send it to law enforcement authorities. It can be argued that, as the online service providers are located in a certain State, the online service provider must meet local regulations, including those that specify how data should be disclosed to law enforcement authorities.

Unilateral data production orders and the Dutch approach

The practice in which online service providers decide themselves whether to voluntarily disclose information may still lead to results that are unsatisfying to law enforcement authorities. This is illustrated by the following Dutch case. In 2012, an unknown individual impersonated a Dutch student and published discriminatory statements in that student's name on Twitter. These statements damaged the reputation of the student, who subsequently sought help from Dutch law enforcement authorities. These authorities can obtain subscriber data from an online service provider such as Twitter. As explained in subsection 2.2.1, an IP address may provide the information required to identify an internet user. When Twitter refused to disclose the information voluntarily, Dutch authorities submitted a legal assistance request to U.S. authorities. However, they did not receive the information because the discriminatory statements were not illegal in the United States. In response to parliamentary questions concerning the case, the Dutch Minister of Security and Justice provided the above facts but took no further action.[42]

In 2011, Belgian law enforcement authorities decided to take a different approach and unilaterally applied a data production order that was regulated in Belgian criminal procedural law in order to obtain data relating to the online service provider Yahoo! Inc.[43] The data production order was sent, because Yahoo! Inc. refused to cooperate and (voluntarily) disclose the information following the data production order. The Belgian courts were greatly divided as to whether the unilateral application of Belgian law was

42 See also J.J. Oerlemans, 'Antwoord Kamervragen over identiteitsfraude VU-studente', *Computerrecht* 2014, no. 1, p. 57-58.

43 For an extensive analysis of the cases, see, e.g., De Hert & Boulet 2012, De Schepper & Verbruggen 2013, Kerkhofs & Van Linthout 2013, and Verbuggen 2014.

allowed in this instance.[44] The judges eventually reasoned that since Yahoo! Inc. offers its services to Belgian citizens, the company is 'located' in Belgium and Belgian law enforcement authorities have jurisdiction to apply local law. The Belgian courts subsequently fined Yahoo! Inc. for not cooperating with the legal order to disclose customer information to Belgian law enforcement authorities under Belgian law.[45]

De Schepper and Verbruggen (2013, p. 161) point out that the Belgian courts essentially ignored the difference between jurisdiction to prescribe and jurisdiction to enforce in international criminal law. Although Belgian law enforcement authorities may be authorised to prescribe their laws to Yahoo! Inc., they are not allowed to *enforce* their criminal procedural laws on foreign companies by imposing fines for non-compliance with Belgian law (cf. Verbruggen 2014, p. 137). The principle of the territorial restriction of enforcement power does not allow States to enforce their laws on foreign territory. It is also questionable whether the fine imposed on Yahoo! Inc. can be enforced in practice. As Yahoo! Inc. does not have any assets or employees in Belgium, the Belgian State does not have the option to use force against persons or companies on its territory to enforce local law (cf. De Schepper & Verbruggen 2013, p. 164). Additionally, foreign courts do not enforce the decisions of another State's criminal court without consent from the competent State authorities. There is thus almost no chance that U.S. courts will fine Yahoo! Inc. in the United States to uphold the Belgian decision to fine the company.

In comparison to Belgium, the Netherlands appears to adopt a more moderate approach. In practice, Dutch law enforcement authorities issue data production orders to foreign online service providers, who then decide whether to voluntarily disclose the requested information. If they opt not to, the authorities will turn to mutual legal assistance. The Dutch legislature emphasises that these procedures 'take a considerable amount of time'.[46] As far as I am able to determine through my research, Dutch law enforcement officials have not issued unilateral data production orders to online service providers. It is also clear that no online service providers were sanctioned by Dutch courts for not disclosing information to Dutch law enforcement authorities.

---

44 See Court of First Instance Dendermonde, 2 March 2009, *Tijdschrift voor Strafrecht* 2009, no. 2, p. 117-120; Court of Appeal Gent, 30 June 2010, *Computerrecht* 2010, no. 6, p. 351; Belgium Supreme Court, 18 January 2011, *AM* 2011, no. 2, p. 218 m. nt. Vandezande; Court of Appeal Brussels, 12 October 2011, *AM* 2012, no. 2-3, p. 238 m. nt. De Schepper, Belgium Supreme Court 4 September 2012, *Digital Evidence and Electronic Signature Law Review* 2013, 10, p. 155-157 m. nt. Vandendriessche; Court of Appeals Antwerpen, 20 November 2013, *Tijdschrift voor Strafrecht* 2014, no. 1, p. 75-76 m. nt. Schoorens.

45 See K. De Schepper, 'Doek valt over Yahoo-zaak', Computerrecht 2016, no. 1, p. 76.

46 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 8-0.

U.S. approach

The United States has a different view on the territorial limits of enforcement jurisdiction when it comes to issuing data production to companies on foreign territory. This State's law enforcement authorities are known for sending data production orders to foreign companies in the event that cooperation through legal assistance is not likely to secure the information they need (cf. Snow 2002, p. 231).

This approach originated in the 1980s, when U.S. law enforcement officials issued data production orders to banks that had local branches or conducted business in the United States and law enforcement officials needed documents that had to be obtained from a branch of these banks on foreign territory.[47] In these cases in the 1980s, U.S. courts determined that:

"the U.S. interest in investigating crime is greater than the foreign interest in bank secrecy and that banks must comply with the subpoenas regardless of the potential hardship they may suffer due to the conflict with foreign law" (Snow 2002, p. 232).

This practice of U.S. courts, which entails conducting a 'balancing of interests' test to decide whether unilateral data production orders are allowed, is rather peculiar from the strict European continental viewpoint on the territorial limitation of enforcement jurisdiction (cf. Maier 1983, p. 584).[48] Scholars from continental Europe generally view this practice as a violation of international law, as it violates both the foreign State's sovereignty and the principle of non-intervention (cf. Ryngaert 2008, p. 80-81). The compelled production of documents stored on foreign territory is viewed as an act of enforcement power that requires consent or a treaty basis for execution (cf. Gercke 2012, p. 277).

The same U.S. practice of unilateral data production orders also currently occurs when data production orders are issued to online service providers. For example, in 2014 Microsoft fought a data production order that U.S. law enforcement authorities sent under U.S. law to obtain stored content data on servers at Microsoft's subsidiary in Ireland.[49] Microsoft had already handed over subscriber data and traffic data to U.S. law enforcement authorities, but it refused to execute the data production order with regard to content data. Microsoft was of the opinion that the information being sought should have been obtained using mutual legal assistance conditions as stipulated in Irish law, stating that Irish law and EU directives apply to

47 See most notably the Nova Scotia cases, U.S. Court of Appeals, 11th Circuit Court 29 November 1982, In re Grand Jury Proceedings (*Bank of Nova Scotia I*), 691 F.2d 1384 (1982) and U.S. Court of Appeals, 11th Circuit Court 14 August 1984, In re Grand Jury Proceedings Bank of Nova Scotia (*Bank of Nova Scotia II*), 740 F.2d 817 (1984).

48 See, e.g., Mann: *"It is difficult to imagine a clearer case in which American legal chauvinism has led to the disregard of elementary rules of international law"* (Mann 1984, p. 52).

49 See Brad Smith, 'We're Fighting the Feds Over Your Email', *The Wall Street Journal* (opinion), 29 July 2014. Available at: http://www.wsj.com/articles/brad-smith-were-fighting-the-feds-over-your-email-1406674616 (last visited on 2 February 2015).

"Hotmail and Outlook.com accounts hosted in Ireland".[50] The U.S. Department of Justice argued that under the Stored Communication Act, the location of the records is irrelevant. The appropriate test for the production of the information is *control of the information*, not the location of the information. In this case, Microsoft employees in the United States could access the data in the United States without the involvement of Irish authorities (see Schwerha IV 2015, p. 10-11). In the first instance of the case, Microsoft was ordered to hand the data stored in Ireland over to U.S. law enforcement authorities. The U.S. court held that the investigative activities took place in the United States when U.S. law enforcement officials reviewed the data. The U.S. also court determined that the relevant question was whether the data was in Microsoft's control. As it was, the information had to be disclosed based on the data production order.[51] In appeal, the U.S. Court of Appeals (2nd Circuit) disagreed and concluded that the Stored Communications Act does not have an extraterritorial reach.[52] The content data is located on servers of a data centre of Microsoft in Ireland. Therefore, using the location of the stored data as a localisation principle, the judges concluded that a U.S. warrant under the Stored Communications Act cannot force Microsoft to send the data from Ireland to the United States.[53] Interestingly, in his concurring opinion, judge Lynch warned that the judgment leads to the dangerous conclusion that the privacy protection of individuals is now in the hands of companies that can simply relocate their infrastructure to avoid complying with the Stored Communication Act.[54] For that reason, he urged that – should the Stored Communications Act be revised – the international reach of the statute should be clarified and balanced against het interests of other sovereign States.[55] The U.S. Department of Justice can go in appeal to the judgment. I expect that when the Stored Communications Act is amended by the U.S. Congress, the statute will be given explicit extraterritorial reach

50 Available at: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/ (last visited on 20 March 2014).

51 See U.S. District Court Southern District of New York, *In re Warrant to Search a Certain E-Mail account Controlled and Maintained by Microsoft Corp*., 25 April 2014, F.Supp.3d 466. See also David Kravets, 'Microsoft ordered to give US customer e-mails stored abroad', *Ars Technica,* 31 July 2014. Available at: http://arstechnica.com/tech-policy/2014/07/microsoft-ordered-to-give-us-customer-e-mails-stored-abroad/ (last visited on 16 January 2015).

52 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Microsoft Corporation v. United States of America, 14 July 2016, p. 42.

53 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Microsoft Corporation v. United States of America, 14 July 2016, p. 39.

54 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Microsoft Corporation v. United States of America, 14 July 2016, conc. J. Lynch, p. 4.

55 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Microsoft Corporation v. United States of America, 14 July 2016, conc. J. Lynch, p. 20.

in order to enable U.S. law enforcement authorities to acquire data from U.S. companies under U.S. regulations. Such a policy will also suit the (Third) Restatement on Foreign Relations Law of the United States, which clearly provides for the possibility that a U.S. company can be compelled to hand data over to U.S. law enforcement authorities, even when that data is stored on foreign territory.[56]

In its *Transborder Access and Jurisdiction* report, the Transborder Group of the Cybercrime Convention Committee of the Council of Europe also affirmed that the United States is of the opinion that it can "*request data from any cloud server located anywhere around the world*", insofar as these online service providers are subject to U.S. jurisdiction.[57] According to the report, U.S. law enforcement authorities assume that an online service provider is subject to U.S. jurisdiction when that entity (1) is based in the United States, (2) has a subsidiary or office in the United States, or (3) otherwise conducts continuous and systematic business in the United States.[58] Based on the report and the abovementioned Restatement it is likely that U.S. will maintain the practice of serving unilateral data production orders if necessary, even when the data is located on foreign territory (cf. De Schepper & Verbruggen 2013, p. 162).[59]

9.3.2 Dangers to legal certainty

This subsection illustrates the dangers to legal certainty that arise when law enforcement officials issue data production orders to foreign online service providers using a brief comparison of relevant Dutch and U.S. regulations.

The Dutch legal framework for data production orders that are issued to online service providers has already been extensively examined in chapter 5. A summary of the results is presented under A below. A brief analysis of the U.S. (federal) regulations for this investigative method is conducted under B. Finally, the most important differences between the two sets of regulations are identified under C.

56 See Restatement (Third) of Foreign Relations Law § 442(1)(a): *"A court of agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, object, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States"* (emphasis added by the author). 'A person' is in practice interpreted as a company that falls under U.S. jurisdiction, even if that company also has an establishment abroad.

57 T-CY 2012, p. 48.

58 T-CY 2012, p. 48.

59 See also Kruijsen 2013, who refers to the U.S. Court of Appeals, 9th Circuit Court, 3 October 2011, *Suzlon Energy, Ltd. v. Microsoft Corporation* (2011), 671 F.3d 726, in which the 9th Circuit Court ordered Microsoft to hand information from an Indian account holder over.

A Overview of Dutch regulations

In the Netherlands, data production orders are regulated by a bipartite legal regime that stipulates in detail the conditions under which (1) electronic communication service providers and (2) all (other) persons, institutions, and companies must disclose information to law enforcement authorities. These authorities can gather the following categories of data using data production orders: (1) subscriber data, (2) traffic data, (3) other data, (4) sensitive data, and (5) content data.[60]

The procedural safeguards that apply to data production orders (i.e., authorisation from a law enforcement official, public prosecutor, or investigative judge) depend on the gravity of the privacy interference that the orders cause. Data production orders that gather subscriber information are regarded as the least intrusive and law enforcement officials are not required to obtain authorisation from a higher authority. Data production orders that gather content data are seen as the most intrusive and require a warrant from an investigative judge.[61] In section 6.3 of chapter 6, stronger procedural requirements were proposed for data production orders in the categories of other data and traffic data in the Netherlands.[62]

B Overview of U.S. regulations

The U.S. regulations for data production orders that are issued to online service providers are examined in B.1, by analysing the Fourth Amendment in relation to the investigative method. The detailed regulations for this investigative method in U.S. criminal procedural law are then explored under B.2.[63]

B.1 Fourth Amendment to the U.S. Constitution

The U.S. Supreme Court has held in several judgments that when information has been 'revealed to a third party' by a citizen, the Fourth Amendment to the U.S. Constitution is not violated if that information is then disclosed by the third party to law enforcement authorities. Any subjective expectation of the involved individual that third parties will keep the information confidential is not relevant (DoJ Manual 2009, p. 8). This exception to the warrant requirement for searching for evidence at a particular place is called the '*third party doctrine*'. The landmark cases of *United States v. Miller*[64] and

60 See section 6.1 of chapter 6.

61 These are visualised in Figure 6.1 in the introduction to chapter 6.

62 See chapter 6 for a more extensive overview.

63 The manual for Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations of the U.S. Department of Justice (DoJ Manual 2009) is also referred to when it provides additional relevant information.

64 U.S. Supreme Court 21 April 1976, *United States v. Miller*, 425 U.S. 435, at 443-444 (1976). In the case of *United States v. Miller*, the U.S. Supreme Court held that the Fourth Amendment does not protect bank account information, because an account holder must assume the risk that the information in control of the third party is conveyed to the government.

Smith v. Maryland[65] established the general rule that when information is in the hands of third parties, an individual lacks a reasonable expectation of privacy with regard to disclosure of that information (Solove 2004, p. 201). Internet service providers are also considered third parties. Lower U.S. courts have confirmed that U.S. citizens have no reasonable expectation of privacy concerning subscriber information that is stored at online service providers (cf. Petrashek 2009, p. 1522).[66]

However, lower courts have recently held that the constitutional protection of the Fourth Amendment does apply to '*stored content information*' that is available at third parties. In the United States, content data is understood as *"any information concerning the substance, purport, or meaning of that communication"*.[67] Most notably, in the case of *Warshak v. the United States*, the U.S. 6th Circuit Court of Appeals decided that the contents of e-mail are protected by the Fourth Amendment.[68] Other (lower) courts subsequently decided that Fourth Amendment protection also applies to other stored content at online service providers, for instance Facebook messages (cf. Kerr 2013, p. 6).[69] Federal legislation has been proposed in the United States, which would require law enforcement officials to obtain a warrant to acquire content data from online service providers by the use of data production orders.[70]

B.2 U.S. criminal procedural law

In 1986, the U.S. Congress created the Stored Communications Act (hereinafter: SCA) to protect personal data that is available at communication

65 U.S. Supreme Court 20 June 1979, *Smith v. Maryland*, 442 U.S. 735, at 743-744 (1979). In the case of *Smith v. Maryland*, the court also held that individuals have no reasonable expectation of privacy in phone numbers dialled by the owner of a telephone, because the act of dialling a number effectively discloses that information to the phone company.

66 See, e.g., U.S. District Court for Connecticut 9 August 2005, *Freedman v. America Online*, 325 F. Supp. 2d 638 (2005) (obtaining subscriber data from the internet access provider AOL): *"In the cases in which the issue has been considered, courts have universally found that, for purposes of the Fourth Amendment, a subscriber does not maintain a reasonable expectation of privacy with respect to his subscriber information"*, U.S. Court of Appeals (10th Circuit) 11 March 2008, *United States v. Perrine*, 518 F.3d 1196, at 1204 (2008) (obtaining subscriber data from Yahoo! Inc with regard to its webmail service and the internet access provider Cox Communications), U.S. Illinois Southern District Court 11 April 2009, *Courtright v. Madigan et al.* (2009) (obtaining subscriber data from social media service MySpace).

67 See 18 U.S.C. § 2510(8).

68 U.S. Court of Appeals (6th Circuit) 14 December 2010, *Warshak v. United States,* 490 F.3d 455 at 266 (2010). Unfortunately for the suspect, the evidence was admissible because the officers relied on good faith on the provisions of the SCA.

69 See, e.g., U.S. District Court of Minnesota, 6 September 2012, *R.S. and S.S. v. Minnewaska Area School*, Dist. No. 2149, F. Supp.2d, p. 29 (2012).

70 See April Glasier, 'It May Soon Be a Lot Harder for the Law to Get Into Your Email', *Wired*, 29 April 2016. Available at: https://www.wired.com/2016/04/finally-might-verge-email-privacy-reform/ (last visited on 24 May 2016).

service providers (cf. Kerr 2004, p. 1212).[71] The SCA regulates the mandatory disclosure of information upon orders from U.S. law enforcement authorities or judges.[72] Under the SCA, U.S. law enforcement officials can use the following three instruments to obtain data: (1) a subpoena, (2) a d-order, and (3) a warrant.

A 'subpoena' is a legal order that compels a third party to disclose data (cf. Kerr 2010, p. 516).[73] The requirements for issuing a subpoena are low (DoJ Manual 2009, p. 128-133). The government must show that the information it seeks is *"relevant to the investigation"* and its production not *"overly burdensome"* (Stuntz 1995, p. 1038).[74]

A 'd-order' derives its name from the legal article on which it is based, namely 18 U.S.C. § 2703(d). This court order specifies the conditions under which online service providers are compelled to disclose information to law enforcement authorities. A d-order can be issued by any federal magistrate from a district court or an equivalent judge from a state court at the request of law enforcement officials.[75] Kerr (2010, p. 514) describes the requirements for obtaining a d-order as "*something of mixture of a subpoena and a search warrant*". Law enforcement officials must provide *"specific and articulable facts showing that there are reasonable grounds to believe"* that the information to be compelled is *"relevant and material to an ongoing criminal investigation."*[76]

A search warrant is a judicial order authorising police to execute a search or seizure under stringent legal thresholds (Kerr 2010, p. 289). Search warrants are only provided by a magistrate judge at request of a law enforcement official. The two conditions to obtain a warrant are (1) 'probable cause' and (2) the particularity requirement. Probable cause means that *"a fair prob-*

---

71 The SCA is part of the broader Electronic Communications Privacy Act of 1986 (hereinafter: ECPA). The ECPA is codified in U.S. federal criminal procedural law in 18 U.S.C. §§ 2701-12.

72 In the United States, information can also be voluntarily disclosed in case (1) the disclosure is made with the lawful consent of the customer or subscriber (which can possibly be derived from terms and conditions), (2) the provider believes in good faith that an emergency involving the danger of death or serious physical injury requires the disclosure without delay, and (3) the disclosure is made to the National Center for Missing and Exploited Children, for instance when child pornography is discovered on a service provider's network (see 18 U.S.C. par 2702(b) and 18 U.S.C. par 2702(c)).

73 With regard to subpoenas, see further LaFave 2009a, p. 7-8 and LaFave 2009b, p. 10. With more extensive regard to grand jury subpoenas, see LaFave 2009a, p. 435-511. The United States also grants a limited subpoena authority to federal law enforcement agencies for the investigation of particular crimes (LaFave 2009a, p. 8). These subpoenas are called 'administrative subpoenas'. For example, the FBI has an administrative subpoena authority in the investigation of drug-related crimes and child abuse cases.

74 Stuntz remarks that courts measure the relevance and burden with a *"heavy thumb on the government's side of the scales"* (Stuntz 1995, p. 1038).

75 See for example 18 U.S.C. §§ 2703(d) and 2711(3).

76 See 18 U.S.C. §§ 2703(d) . The 'specific and articulable facts' standard derives from the U.S. Supreme Court's decision in U.S. Supreme Court 10 June 1968, *Terry v. Ohio*, 392 U.S. 1 (1968), p. 21. See also U.S. Court of Appeals (10th Circuit) 11 March 2008, *United States v. Perrine*, 518 F.3d 1196, at 1202 (2008).

ability exists that contraband or evidence of a crime will be found in a particular place" (DoJ Manual 2009, p. 64).[77] In the context of digital evidence, the particularity requirement means that law enforcement officials must describe which information is being sought where. A warrant should describe how to separate relevant from irrelevant items. In addition, the evidence that is looked for must be limited to the scope of the probable cause established in the search warrant (DoJ Manual 2009, p. 69-70).

The categories of data production orders that can be issued to online service providers (as distinguished in this study) are further examined below.[78]

Subscriber and traffic data

The SCA specifies that a subpoena can be issued to enable U.S. law enforcement officials to obtain both subscriber and traffic data from online service providers. The scope of the data production order is restricted by a limited list of data.[79] The following data can be obtained from a subscriber under this legal basis: (a) name, (b) address, (c) records of session times and durations of a communication, (d) length of service (including start data) and types of services, (e) other subscriber number or identity (such as an IP address), and (f) means of payment for such service. This is reflected in policies of online service providers, such as Google, that state on their website how they handle data production orders that are send to them by law enforcement authorities.

For example, Google states on its website that with regard to its webmail service Gmail, law enforcement officials can request the following information with a valid subpoena: (1) subscriber registration information (e.g., name, account creation information, associated e-mail addresses, phone number) and (2) sign-in IP addresses and associated time stamps.[80]

Other data

In the United States, law enforcement officials can obtain other data – i.e., data that does not fall into the subscriber, traffic, or content categories – from online service providers using a d-order. To make this category of data more

77 The standard has been defined *"as where the facts and circumstances within the officer's knowledge are sufficient in themselves to warrant a person of reasonable prudence to belief that contraband or evidence of a crime will be found in a particular place or on a particular person"* (U.S. Supreme Court 2 March 1925, *Carroll v. United States*, 267 U.S. 132, at 162 (1925).

78 In the United States, there is also ambiguity with regard to exactly which SCA regulations apply to online service providers, as the legal orders are differentiated between 'electronic communication service providers' and 'remote storage providers'. For readability, only the term 'online service providers' is used. This simplifies the U.S. legal framework to some extent. However, the essence of the regulations and their accompanying procedural safeguards remains unchanged.

79 See 18 U.S.C. § 2703(c)(2).

80 See https://www.google.com/transparencyreport/userdatarequests/legalprocess (last visited on 30 April 2016).

concrete an example is given. Google states on their website that the company provides following information under a valid d-order:

"a government agency can obtain the same information as a subpoena, plus more detailed information about the use of the account. This could include the IP address associated with a particular email sent from that account or used to change the account password (with dates and times), and the non-content portion of email headers such as the "from," "to" and "date" fields. An ECPA court order is available only for criminal investigations."[81]

Content data

The category of content data is ill defined in U.S. law. Kerr (2004, p. 1228) explains that the SCA refers to the U.S. Wiretap Act for the definition of content information. However, that definition "only states what it includes, not what it actually is" (Kerr 2004, p. 1228). The Wiretap Act specifies that content information 'includes any information concerning the substance, purport, or meaning of communications'.[82] Content data involves electronically stored communications and clearly includes e-mails that are available at online service providers, but it remains unclear what other data is considered content data (cf. Kerr 2013). In this respect, it is notable that online service providers such as Google already state on their websites that they require a warrant not just for e-mail, but also for "search query information" and "private content stored in a Google Account, such as Gmail messages, documents, photos and YouTube videos".[83]

The U.S. regulations for obtaining content data from online service providers are particularly complex.[84] For the purposes of this study and comparison, it is most important to note that e-mails that are more than 180 days old can be obtained with either a subpoena or d-order,[85] while a SCA warrant is required for e-mails that are 180 days old or less.[86]

When a warrant is executed under the SCA, *"all e-mails from within an email account"* are handed over to the investigators *"who then identify and copy information that fall within the scope of the particularized 'items to be seized' under the warrant"* (DoJ Manual 2009, p. 134).[87] It is debatable whether the

81 See https://www.google.com/transparencyreport/userdatarequests/legalprocess/ (last visited on 30 April 2016).

82 See 18 U.S.C. § 2510(8).

83 See https://www.google.com/transparencyreport/userdatarequests/legalprocess/ (last visited on 30 April 2016).

84 For an extensive analysis, see, e.g., Kerr 2004 and Kerr 2010.

85 See 18 U.S.C. § 2703(b)(1)(b)(i) and 18 U.S.C. §2703(b)(1)(b)(ii).

86 See 18 U.S.C. §2703(a)

87 See also Brid-Aine Parnell, 'US judge: YES, cops or feds SO CAN SLURP an ENTIRE Gmail account', *The Register*, 21 July 2014. Available at: http://www.theregister.co.uk/2014/07/21/judge_okays_cops_slurping_entire_email_account/ (last visited on 21 July 2014). The is called a '2703-warrant', derived from its legal basis in 18 U.S.C. § 2703.

disclosure of an entire e-mail account meets the 'particularity requirement' of a warrant.

As explained above, there is a trend in case law that content data available at third parties can only be collected with a warrant. In addition, congressional legislation that would amend the SCA to require a warrant for content data has been proposed.

C Notable differences

From a fundamental rights perspective, the most notable difference between Dutch and U.S. law in the context of data production orders is that individuals in the Netherlands are protected by the right to privacy as articulated in art. 8 ECHR when online service providers disclose data that they store to law enforcement officials. In the United States, individuals are not protected by the warrant requirement of the Fourth Amendment for information that is available at online service providers, due to the third party doctrine. Lower U.S. courts have however recently provided Fourth Amendment protection to content data stored at online service providers, although the scope of what content data entails and the protection that it is currently provided in practice remain unclear.

Nevertheless, the regulations for using data production orders to obtain data from online service providers are essentially similar in the Netherlands and the United States. The criminal procedural laws in both States contain detailed regulations that protect personal information from individuals that is stored at online service providers. In addition, both States differentiate data production orders on the basis of the orders' sensitivity. This is done in a similar manner, although more types of data production orders are regulated in detail as investigative powers in the Netherlands. In addition, it is clear that in the Netherlands, stored e-mails available at an online service provider can only be obtained with a warrant.

However, these similar regulations are not identical and differences can still endanger the legal certainty of the individuals involved. For example, Google states on its website that it can voluntarily disclose information to non-U.S. law enforcement authorities "*if those requests are consistent with international norms, U.S. law, Google's policies and the law of the requesting country.*"[88] However, exactly what "Google's policies" entail is not public.[89] For instance, what if Brazilian law enforcement authorities request data from U.S. online service providers concerning an individual located on Dutch territory? Will information be disclosed based on Brazilian criminal

88 Available at: https://www.google.com/transparencyreport/userdatarequests/legalprocess/ (last visited on 30 July 2015).

89 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 9: *"The transparency reports by companies such as Google and Microsoft provide insufficient information about the willingness of companies to cooperate [by voluntarily disclosing data to Dutch law enforcement officials] and do not specify the origin and legal basis [of data production orders]."*

procedural law, Dutch criminal procedural law, or U.S. criminal procedural law? Online service providers may experience a conflict of regulations in this situation.

Practice also shows that U.S. law enforcement authorities send data production orders unilaterally across State borders to online service providers to obtain data that is located outside U.S. territory. The legal certainty of individuals is endangered when that data belongs to individuals who do not reside in the United States. At the same time, individuals should – in my view – realise that when they make use of U.S. online services, U.S. law enforcement authorities can obtain their information under U.S. law.[90] The practice of issuing cross-border unilateral data production orders to online service providers becomes especially problematic in terms of both State sovereignty and legal certainty, when data production orders are issued to online service providers that are located on foreign territory (as well as their infrastructure).

9.3.3 Section conclusion

Online service providers can potentially offer their services to individuals who are located all over the world. At the moment, U.S. online services are particularly popular. Non-U.S. law enforcement authorities, including Dutch law enforcement authorities, want to be able to gather evidence that is located at these online service providers. A practice has emerged in which online service providers voluntarily disclose information to foreign law enforcement authorities after receiving data production orders, even when that information is potentially physically located in a data centre on foreign territory.

Dutch law enforcement authorities follow this practice. There are no indications that they unilaterally issue data production orders across State borders and force these providers to disclosure data under the threat of a fine if they do not cooperate. Foreign online service providers decide themselves whether to disclose data voluntarily. If the data is not voluntarily disclosed, mutual legal assistance procedures must be used to gather the data. Online service providers may experience conflicting obligations caused by regulations, when foreign law enforcement officials issue a data production order or the data relates to an individual that is located on foreign territory. In this situation, the legal certainty of the individual involved is also endangered.

---

90 After the latest Microsoft Ireland decision (U.S. Court of Appeals District Court of Connecticut (2nd Circuit) 14 July 2016, *Microsoft Corporation v. United States of America* (In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation), this is only true for non-content information. However, in my view it is likely the decision will be overturned by a different U.S. Court or the SCA will be amended to allow for an extraterritorial application. This belief is founded by the examined previous case law with regard to bank records and the policy formulated in the Restatement (Third) of Foreign Relations Law.

U.S. law enforcement authorities do send data production orders unilaterally across State borders to online service providers that potentially store their data on foreign territory. This practice is understandable for U.S. online service providers. These online service providers are regulated by the United States. The cross-border unilateral issuance of data production orders to foreign companies that only provide services to U.S. residents, without assets in the United States, is more problematic in terms of both State sovereignty and legal certainty.

No treaty basis is available for either the voluntarily or mandatory disclosure of information by online service providers after the cross-border unilateral issuance of data production orders. It can therefore be argued that this practice is in violation of international law. However, the practice can be explained by the popularity and large growth of online services in the last decade, which has led to law enforcement authorities wanting to obtain data from these online service providers in an efficient manner. The practice endangers the legal certainty of the individuals involved, since it is unclear under which conditions – and even which laws – online service providers disclose information to foreign law enforcement authorities.

9.4 Online undercover investigations

The section examines the consequences of cross-border unilateral undercover investigations. Section 9.4.1 explores what the Netherlands and the United States think about desirable restrictions for the cross-border unilateral application of the investigative method. Section 9.4.2 then compares how the two States have regulated this method to identify the regulatory differences that illustrate the dangers to legal certainty. A section conclusion is provided in subsection 9.4.3.

9.4.1 Interferences with territorial sovereignty

The territorial limitation of enforcement jurisdiction leads to the restriction that investigative methods can only be applied within the borders of State, insofar as no permission is obtained from the other State and no treaty basis that authorises the evidence-gathering activity is available. Brownlie describes this principle as follows:

"Persons may not be arrested, a summons may not be served, police or tax investigations may not be mounted, orders for production of documents may not be executed, except under the consent of a treaty or other consent given" (Crawford 2012, p. 479).

The Netherlands is of the opinion that this territorial limitation of enforcement jurisdiction also applies to undercover investigative methods. The use of investigative methods to gather evidence in criminal cases is not allowed

outside of Dutch territory without permission from the involved State(s) or a legal basis in a treaty (cf. Klip 1995, p. 1057).[91] Vice versa, only Dutch law enforcement officials are entitled to use investigative methods on Dutch soil in order to gather evidence in criminal investigations (cf. Klip 1995, p. 1066). The use of investigative methods includes undercover investigative methods, which are regulated in detail in Dutch criminal procedural law. For that reason, the Netherlands did not approve the extraterritorial undercover operations conducted by U.S. Drug Enforcement Administration (DEA) agents on Dutch territory in the 1980s and 1990s (cf. Klip 1995, p. 1068, Van der Wilt 2000 p. 176, and Koers 2001, p. 399).[92] It regarded the extraterritorial evidence-gathering activities of U.S. law enforcement officials in the physical world as a violation of Dutch territorial sovereignty. The Netherlands considers undercover investigative methods as an intrusive investigative method, but not as intrusive as a search at a place or computer hacking.[93]

The Internet makes it particularly straightforward to apply undercover investigative methods across State borders. The Internet enables a law enforcement official to interact with an individual who can be located anywhere in the world. Law enforcement officials no longer have to physically cross State borders to conduct an extraterritorial undercover operation. The extraterritorial effects of online undercover operations must be localised based on where the affected individual resides. Following the territorial restriction of enforcement jurisdiction, it can be argued that permission must be obtained from the State where the individual is located or a relevant treaty basis must be available for the cross-border unilateral evidence-gathering activity (cf. Siemerink 2000a, p. 69).

---

91 See *Kamerstukken II* (Parliamentary Series Second Chamber) 1990/91, 22 142, no. 3, p. 10. While referring to art. 539a DCCP, the legislature at the time explained that the use of *"penal enforcement power outside a State's territory is only allowed with consent of the foreign State"* (translated from Dutch). See also, *Kamerstukken II* (Parliamentary Series Second Chamber) 1985/86, 19 328, no. 1, p. 3: *"It is unacceptable when foreign informants operate outside the supervision of (Dutch) law enforcement authorities on Dutch territory"* (translated from Dutch). This statement is repeated in *Kamerstukken II* (Parliamentary Series Second Chamber) 1990/91, 21800VI, no. 39, p. 16. See also Rb. Amsterdam, 27 April 2007, ECLI:NL:RBAMS:2007:BA4017. See for a more recent example, answers to questions of parliamentary member Nispen regarding an U.S. undercover operation in the Netherlands, 4 July 2016, no. 2016Z11467: *"The mutual legal assistance treaty between the United States and the Netherlands prescribes that mutual legal assistance is required to conduct investigative activities on each other's territory"* and "*It is a well-known principle in international law that law enforcement officials are not allowed to conduct investigative activities on another State's territory without permission"* (translated by the author).

92 See answers to questions of parliamentary member De Wit regarding foreign law enforcement authorities, 19 March 2007, no. 5474459/07. The Dutch Minister of Security and Justice at the time formally protested to his U.S. counterpart about the unilateral operation of the DEA on Dutch territory in 2007 (see Rb. Amsterdam, 27 April 2007, ECLI:NL:RBAMS:2007:BA4017). The minister also made arrangements with the DEA to prevent such behaviour in the future.

93 See the analysis in chapter 7 and 8 regarding the regulation of these investigative methods in the Netherlands.

It is expected that the Netherlands views the cross-border unilateral application of online undercover investigative methods that involve foreign individuals as acceptable only insofar as permission is obtained from the affected State or a treaty basis that authorises the evidence-gathering activity is available. When a treaty regulates the application of undercover investigative methods on the territory of a different State in the physical world, the relevant treaty provision also applies to the online application of undercover investigative methods.

However, circumstances may exist in which the cross-border unilateral application of online undercover investigative methods that involve foreign individuals is acceptable from a Dutch (and continental) law perspective. When the individual involved in a criminal investigation uses a nickname and an IP address is not available as a (usable) digital lead (for example because these individuals are utilising Tor or other anonymising services), the extraterritorial effects of the undercover operation cannot be localised. In this situation, the principle of the territorial application of enforcement power cannot be applied. As a result, it can be argued that cross-border unilateral online undercover investigative operations are acceptable when the location of the individuals involved cannot be reasonably determined (cf. O'Floinn & Ormerod 2011). For example, in a U.S. undercover operation conducted by the DEA, U.S. law enforcement officials reportedly bought drugs that was offered by on an advertisement by an individual with the nickname 'adamsflower' on the website 'pharmacyrater.com'. This evidence-gathering activity constitutes a pseudo-purchase in the Netherlands, which requires the application of the special investigative power of a pseudo-purchase that can be authorised by a public prosecutor for the investigation of crimes defined in art. 67 DCCP. Eventually, the suspect was traced down to his residence in the Netherlands by U.S. law enforcement authorities and arrested by Dutch law enforcement authorities upon request. He was extradited to the United States in 2014. After almost two years, he was returned to the Netherlands to serve the remainder of his sentence.[94] The case led to controversy in the Netherlands, because U.S. law enforcement authorities were accused of conducting an undercover operation in the Netherlands without permission of the Dutch State and using an illegitimate form of entrapment for the online pseudo-purchase. The Dutch Minister of Security and Justice stated in response to parliamentary questions that U.S. law enforcement officials can conduct an online pseudo-purchase of drugs that are offered by 'a global anonymous online crime organisation', even when it becomes clear *after* the operation that the individual that sold the drugs was located on Dutch ter-

94 See Tom Kreling & Huib Modderkolk, 'De dealer die in de Amerikaanse val werd gelokt', *De Volkskrant*, 7 June 2016. The journalists state (based on court documents) that U.S. law enforcement authorities already knew the suspects location, since subscriber data and e-mails were obtained from the Canadian webmail service 'Hushmail'. The Dutch suspect may have also been identifiable by subscriber data and traffic data available at the online payment service PayPal and the money transmitting service Western Union.

ritory.[95] The Dutch Minister also (rightfully) explained that with regard to the pseudo-purchase no entrapment had taken place, since the goods were already offered on a website by the suspect. As will be further explained in subsection 9.4.2, the concept of entrapment in the Netherlands and United States differ. Therefore, the application of online pseudo-purchase could be problematic when law enforcement officials have many interactions with the suspect prior to the pseudo-purchase. The undercover operation does raise the question to which extent these operations can take place and at which point in the investigation law enforcement officials must attempt to localise the suspects. For example, law enforcement officials can attempt to localise individuals by sending data production orders to obtain subscriber data from online services that the involved individuals utilise. As soon as the location of the individual is known, mutual legal assistance should be used to conduct evidence-gathering activities with extraterritorial effects on foreign territory.

In addition, different investigative methods may interfere with State sovereignty at different levels of severity. In chapter 7, online undercover investigative methods were distinguished as (1) online pseudo-purchases, (2) online interactions with individuals, and (3) online infiltration operations. When online pseudo-purchases and online infiltration operations are applied, undercover agents commit authorised crimes. These investigative methods may be regarded as a violation of the affected State's territorial sovereignty when no permission is provided by the affected State to conduct the (often minor) crime on its territory (cf. O'Floinn & Ormerod 2011). Online interactions with individuals may be regarded as less intrusive investigative methods, since they only involve law enforcement officials interacting with individuals in an undercover capacity. States may find this type of online undercover operations (in which no crimes are committed) being undertaken on their territory without their permission as more acceptable. Interestingly, the individuals involved may regard these online interactions as more privacy intrusive than, for example, online pseudo-purchases by law enforcement officials.

However, no formal policy is available that indicates how Dutch law enforcement authorities take the territorial restriction of enforcement jurisdiction into consideration in the context of undercover investigative methods. Based on the Dutch interpretation of the territorial restriction of undercover operations in the physical world, it follows that online undercover investigations are also restricted to the territory of the Netherlands.

95 See answers to questions of parliamentary member Nispen regarding an U.S. undercover operation in the Netherlands, 4 July 2016, no. 2016Z11467. Confusingly, the Minister of Security and Justice also stated that 'no investigative activities took place on Dutch territory'. In my view, evidence-gathering activities factually did take place on Dutch territory. However, it is possible that in first instance, no permission of the Dutch State could be obtained since the location of the individual involved was unclear. The minister informs Dutch parliament that mutual legal assistance has been obtained by U.S. law enforcement officials for the application of other investigative methods.

The territorial effects of the investigative method can be localised using an individual's location. Unless, of course, his location cannot be reasonably determined. It is conceivable that in this situation it is possible to apply online undercover investigative methods unilaterally across State borders, as is also supported by the above mentioned examined letter send to Dutch Parliament.

U.S. approach

Historically, U.S. law enforcement authorities have been more willing than other States to gather evidence across their own State borders by applying cross-border unilateral undercover investigations. Nadelmann (1993, p. 472) aptly describes the U.S. attitude as follows:

"Among the features that distinguish US international law enforcement behavior from that of most other states, however, are the relatively high number of endeavors in which US officials act unilaterally and coercively. No other government has acted so aggressively in collecting evidence from foreign jurisdictions, apprehending fugitives from abroad, indicting foreign officials in its own courts, targeting foreign government corruption, and persuading foreign governments to change their criminal justice norms to better accord with its own."

Indeed, the United States appears to have a view on the territorial restrictions of undercover investigation activities that differs from views held by other States, including the Netherlands.[96] In particular with regard to undercover investigative methods, a possible explanation for the willingness of the United States to conduct undercover operations on foreign territory is that U.S. law enforcement authorities do not view undercover operations as privacy-infringing activities.[97] The analysis in subsection 9.4.2 below further examines the differences between U.S. and Dutch regulations in relation to undercover investigative methods.

The questions are of course whether U.S. law enforcement authorities still conduct undercover operations on foreign territory and whether this practice is continued in an online context. The United States has greatly increased its number of mutual legal assistance treaties with other States since the 1980s. These treaties should facilitate extraterritorial evidence-gathering activities, including undercover operations, which are undertaken by local law enforcement authorities in the physical world (cf. Snow 2002, p. 211). As argued above, these treaties should be interpreted similarly in an online context. However, it may occur that the extraterritorial effects of undercover operations cannot be localised and thus States cannot be not

96 See also Klip 1995, p. 1068, Hoffer 2000, Van der Wilt 2000, p. 176 and Koers 2001, p. 399.

97 Koers (2001, p. 400) points to the one-sided and perhaps hypocritical approach of the United States regarding these unilateral extraterritorial investigation measures, since article 18 U.S.C. § 951 dictates that foreign law enforcement officials are not authorised to conduct investigations on U.S. territory under sanction of a prison sentence.

asked for permission. It is also possible that a different localisation method is used or that individual law enforcement officials simply overstep their boundaries and engage in extraterritorial undercover evidence-gathering activities without consulting on their actions with the appropriate authorities.

The case of David Schrooten illustrates how an online undercover operation can take place in practice.[98] This case also illustrates how these operations can produce extraterritorial effects that potentially interfere with the territorial sovereignty of a State (here the Netherlands) and clearly interfere with the legal certainty of the individual involved. The case is further examined below.

The U.S. Secret Service suspected David Schrooten, a Dutch national, of credit card fraud that involved U.S. victims.[99] At trial, Schrooten's defence counsel stated that the Secret Service had assumed the online identity of a suspect who had been apprehended in the United States and had subsequently used his online account to interact with Schrooten (who was in the Netherlands) in an undercover capacity via the Internet.[100] As explained under C in subsection 2.2.2, the power of law enforcement officials to take over a person's online identity is a unique feature of online undercover operations. The Secret Service agents then purchased credit card numbers from Schrooten, who used the nickname 'Fortezza' on the Internet. Thereby, an online pseudo-purchase as an investigative method was conducted, which requires the application of a special investigative power in the Netherlands by local law enforcement officials or permission of the Dutch State to conduct the online pseudo-purchase. The U.S. law enforcement officials maintained contact with David Schrooten. At one point in the investigation, the suspect flew to Romania to visit his girlfriend. When he arrived, Schrooten was arrested at the airport by Romanian authorities and extradited to the United States. Schrooten was ultimately incarcerated in a U.S. prison after a plea bargain agreement with a U.S. public prosecutor.[101] He eventually returned to the Netherlands to serve the remainder of his sentence in a

98 In the Netherlands, it is not appropriate to indicate the full name of an individual that has been involved in a criminal investigation. However, Schrooten and a journalist co-authored a book about the events (i.e., David Schrooten and Freke Vuijst, *Alias Fortezza*, Balans 2016) and sought media out to tell the story. In this case, I thus assume it is appropriate to mention Schrooten's full name.

99 See the indictment of *United States v. David Schrooten*. Available at: http://krebsonsecurity.com/wp-content/uploads/2012/06/Schrootenindictment.pdf (last visited on 15 April 2016).

100 See the letter of Defence Counsel Stapert. Available at: http://blogs.vn.nl/download/Brief%20Opstelten-Teeven_3.pdf (last visited on 29 January 2015). See David Schrooten and Freke Vuijst, *Alias Fortezza*, Balans 2016.

101 See Harry Lensink and Freke Vuijst, 'Geen krediet voor David S.', *Vrij Nederland*, 15 April 2013. Available at: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Geen-krediet-voor-David-S.-2.htm (last visited on 3 February 2015).

Dutch prison.[102] The conversion of his sentence to the (much lower) Dutch sentence for the crimes led him to being released soon after his arrival back in the Netherlands.

This case created controversy in the Netherlands, partially due to Schrooten's living conditions in the U.S. prison and the manner in which U.S. law enforcement officials obtained his custody. However, the question also arose as to whether U.S. law enforcement officials had engaged in evidence-gathering activities on Dutch territory and lured Schrooten in order to prosecute him, thereby infringing Dutch sovereignty. In response to parliamentary questions, the Dutch Minister of Security and Justice explained that the Netherlands was aware of U.S. law enforcement authorities' interest in Schrooten, but not of any investigative activities that these authorities were undertaking on Dutch territory.[103] In a 2013 letter to Dutch Parliament the minister stated, similar to the above mentioned letter of 2016 regarding the online pseudo-purchase by DEA agents from an Dutch online drugs dealer, that "no investigative measures have taken place on Dutch territory and no permission was therefore required".[104] This was a remarkable statement, as it was unlikely that U.S. law enforcement authorities were able to obtain necessary evidence against the Dutch suspect and coordinate the extradition by Romanian authorities without conducting any investigative activities on Dutch territory. U.S. law enforcement authorities must have applied the special investigative powers for (1) pseudo-purchase and (2) systematic information gathering on Dutch territory to gather the required evidence. The United States did send the Netherlands a mutual legal assistance request regarding investigation measures in the Netherlands *after* Romania had extradited Schrooten to the United States.[105] It was not specified in the letter which investigative methods the mutual assistance request involved.

---

102 See Harry Lensink, 'Minister wil terugkeer hacker David S. bespoedigen', *Vrij Nederland*, 15 April 2013. Available at: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Minister-wil-terugkeer-hacker-David-S.-bespoedigen.htm (last visited on 29 January 2015).

103 See answers to the parliamentary questions of parliamentary member Van Bommel by the State Secretary of Security and Justice regarding the extradition by Romania of Dutch hacker David S. to the United States on 1 August 2012. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2012/08/01/antwoorden-kamervragen-over-de-uitlevering-van-een-nederlandse-hacker-aan-de-vs-door-roemenie (last visited on 26 October 2015).

104 See answers to parliamentary questions on 12 April 2013, regarding the article 'FBI-agenten hacken mee met Nederlandse politie' and the conditions regarding detention in the United States. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2013/04/16/antwoorden-kamervragen-over-fbi-agenten-hacken-mee-met-nederlandse-politie-en-dententieomstandigheden-vs (last visited on 26 October 2015). See also Harry Lensink and Freke Vuijst, 'Geen krediet voor David S.', Vrij Nederland, 15 April 2013. Available at: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Geen-krediet-voor-David-S.-2.htm (last visited on 3 February 2015).

105 See answers to parliamentary questions of parliamentary member Van Bommel by the State Secretary of Security and Justice on 1 August 2012, regarding the extradition by Romania of Dutch hacker David S. to the United States.

It is possible that U.S. law enforcement officials were not aware of Schrooten's identity and location at the time the undercover investigation took place. His nickname, 'Fortezza', alone did not indicate where he was located. Following their online undercover interactions with the suspect, it can be argued that U.S. law enforcement authorities seized the opportunity to request Romania to extradite him once it became clear that he would land at the airport in that country. It can also be argued that U.S. law enforcement officials already knew the identity of Schrooten and should have requested the Netherlands to prosecute or extradite him. Schrooten himself beliefs that U.S. law enforcement authorities were aware of his location and identity. He claimed that the Secret Service obtained this information based on subscriber information from online service providers and financial transactions that he conducted with the money transmitting service Western Union.[106] It also appears that Russian hackers had previously exposed his identity in online forums, which information may have been gathered by U.S. law enforcement officials.[107]

Regardless of which of these two versions of the extraterritorial evidence-gathering activities in the Netherlands is accurate, the case of David Schrooten illustrates how online undercover investigative methods are used and may lead to questions with regard to both the territorial sovereignty of States and the legal certainty of the individual involved. The case shows how U.S. law enforcement officials factually conducted an online undercover operation that involved a Dutch citizen without requesting prior permission from the Netherlands to conduct the operation or having authorisation derived from a treaty.[108] This means that U.S. laws were applied. As U.S. laws for undercover investigative methods are neither accessible nor foreseeable to Dutch citizens, such a practice endangers the legal certainty of the individuals involved. This case also shows how the cross-border unilateral application of online undercover investigative methods can lead to tension concerning another State's territorial sovereignty.

9.4.2 Dangers to legal certainty

The dangers to the legal certainty of the cross-border unilateral application of online undercover investigative method were illustrated above using the case of David Schrooten. In this case, U.S. regulations for undercover investigative methods were applied that interfered with the rights and freedoms of a Dutch citizen. These regulations were not accessible or foreseeable to

106 See David Schrooten and Freke Vuijst, *Alias Fortezza*, Balans 2016, p. 42.

107 See Brian Krebs, 'Feds Arrest 'Kurupt' Carding Kingpin?', KrebsonSecurity blog, 12 June 2012. Available at: http://krebsonsecurity.com/2012/06/feds-arrest-kurupt-carding-kingpin/ and http://krebsonsecurity.com/wp-content/uploads/2012/06/kuruptru.png (last visited on 15 April 2015).

108 Again, this may be explained by the argument that U.S. law enforcement officials were not aware of Schrooten's identity and location.

Schrooten. In other words, his legal certainty was endangered and an arbitrary interference with his privacy took place. Public sources and case law indicate that U.S. law enforcement authorities extensively use undercover investigative methods in an online context.[109] However, these sources and cases do not indicate that U.S. law enforcement authorities deliberately engage in extraterritorial evidence-gathering activities. It is unclear whether they were aware where the suspect was located. It is only clear that they also apply undercover investigative methods in an online context.

This subsection highlights differences in regulations for undercover investigative methods by briefly comparing the current regulations for undercover investigative methods in the Netherlands and the United States. The Dutch legal framework for undercover investigative methods has already been examined extensively in chapter 7. A summary of the results of that analysis is provided under A below. A brief analysis of the U.S. (federal) regulations for the investigative method is then presented under B. Finally, the most important differences between these regulations are identified under C.

A Overview of Dutch regulations

Certain undercover investigative methods are regulated in detail in Dutch criminal procedural law. Undercover investigative methods are generally viewed as interfering with the right to privacy. Those undercover investigative methods that interfere with the right to privacy in a more than minor manner or threaten the integrity of criminal investigations are regulated as special investigative powers in Dutch law. The number of procedural safeguards that apply depends on how intrusive the investigative power is and the risks they pose to the integrity of investigation.

The analysis in chapter 7 showed that online pseudo-purchases are regulated by the special investigative power for pseudo-purchases in criminal

109 See, e.g., U.S. Department of Justice Office of Public Affairs, 'Alleged International Credit Card Trafficker Arrested in France on U.S. Charges Related to Sale of Stolen Card Data', 11 August 2010. Available at: http://www.fbi.gov/atlanta/press-releases/2010/at081110.htm, Kevin Poulsen, 'The Secret Service Agent Who Collared Cybercrooks by Selling Them Fake IDs', *Wired*, 22 July 2013. Available at: http://www.wired.com/2013/07/open-market/ and Kari Paul, 'An Undercover Agent Was Making $1000 a Week in Bitcoin as a Silk Road Admin', *Motherboard*, 14 January 2015. Available at: http://motherboard.vice.com/read/cirrus-bitcoin-buck. All websites last visited on 30 July 2015. See also, e.g., the FBI press release, 'Child Predators. The Online Threat Continues to Grow', 17 May 2011. Available at: https://www.fbi.gov/news/stories/2011/may/predators_051711 (last visited on 17 July 2015). See also the following extract from the press release: "*During investigations, agents sometimes pose online as teens to infiltrate paedophile networks and to gather evidence by downloading files that are indicative of child pornography. During the investigation of known suspects, undercover agents may also 'friend' people the suspect is associated with*". Case law is referred to in this section under B.1.

procedural law. Authorisation from a public prosecutor is required to apply this special investigative power.[110]

Online undercover interactions with individuals derive from either the general legal basis in art. 3 of the Dutch Police Act or the detailed regulations concerning the special investigative power for systematic information gathering. The analysis in chapter 7 showed that ambiguity exists with regard to when this investigative method is considered to be 'systematically' applied and thus requires the application of the special investigative power. In addition, it was argued that the procedural safeguard for the special investigative power of authorisation from a public prosecutor is not sufficient. Instead, it is preferable that both authorisation from a public prosecutor and supervision by an investigative judge are required, due to the investigative method's intrusiveness vis-à-vis privacy interferences and risks regarding the investigation's integrity, given that entrapment may occur. Dutch law enforcement officials must ensure that a civilian does not commit a crime that he would not have committed without the intervention of law enforcement authorities.

Online infiltration as an investigative method is regulated by the special investigative power for infiltration in the Netherlands. This investigative power is different from systematic information in the sense that it authorises law enforcement officials to participate in a criminal organisation and commit certain crimes when necessary. It was argued that Dutch law should also introduce the mandatory supervision of an investigative judge for the special investigative power for infiltration.[111]

B Overview of U.S. regulations

The U.S. regulations for online undercover investigative methods are first examined with regard to the Fourth Amendment to the U.S. Constitution under B.1. This analysis determines whether a warrant is required to apply undercover investigative methods. As no criminal procedural regulations are applicable to these investigative methods, the most relevant and available internal guidelines for (federal) U.S. law enforcement authorities are examined in B.2 to determine the scope of the methods and the manner in which they are applied.

B.1 Fourth Amendment to the U.S. Constitution

The U.S. Supreme Court has decided in several important cases that the Fourth Amendment does not apply with regard to undercover investigative

110 Although the examined case law in subsection 7.2.1 also revealed that, in practice, an online pseudo-purchase is sometimes applied upon the basis of art. 3 of the Dutch Police Act and authorisation by a public prosecutor is not obtained or too late in the investigation.

111 See chapter 7. Figure 7.1 in the introduction to that chapter visualises the intrusiveness of the investigative method according to Dutch law, with the detail of the law and procedural safeguards that currently apply as regulations for the investigative methods.

methods that are applied by U.S. law enforcement officials.[112] These cases lead to the conclusion that U.S. citizens do not have a reasonable expectation of privacy when they interact with other individuals and must assume that those with whom they are communicating may be law enforcement officials. As such, no warrant is required for undercover operations.

The doctrine that individuals do not have reasonable expectation of privacy when they voluntarily disclose incriminating information to another person is called the '*misplaced trust doctrine*' (cf. Petrashek 2010, p. 1528).[113] The doctrine also applies in an online context. For example, the misplaced trust doctrine permits U.S. law enforcement officials to add themselves as a friend to the Facebook profile of a suspect, or the friends of a suspect, in order to obtain private information about that suspect without a warrant (cf. Semitsu 2011, p. 346 and Petrashek 2010, p. 1528). Several U.S. courts also authorised U.S. law enforcement officials to pose as a minor in chat rooms in order to gather evidence about suspects of online child abuse crimes (see Global Information Sharing Initiative 2013, p. 23).[114]

As stated above, no regulations in U.S. criminal procedural law restrict the application of undercover investigative methods by (federal) law enforcement authorities. Ross (2007, p. 511) explains that undercover investigative methods are instead restricted by (1) internal guidelines of U.S. law enforcement authorities, (2) ethical rules for prosecutors (which forbid undercover contacts with suspects that already have a lawyer), and (3) the prohibition of entrapment.

---

112 See, most notably, U.S. Supreme Court 27 May 1963, *Lopez v. United States*, 373 U.S. at 427 (1963), U.S. Supreme Court 12 December 1966, *Lewis v. United States*, 385 U.S. at 206 (1966) and U.S. Supreme Court 12 December 1966, *Hoffa v. United States*, 385 U.S. at 293 (1966) and U.S. Supreme Court 20 October 1970, *United States v. White*, 401 U.S. at 745 (1971). See Maclin 1996 for a historical analysis of case law with regard to the Fourth Amendment and undercover investigative methods.

113 See also U.S. Supreme Court 12 December 1966, *Hoffa v. United States*, 385 U.S at 302 stating that the Fourth Amendment does not protect *"a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"*.

114 See, e.g., U.S. Superior Court of Pennsylvania 28 march 2001, *Commonwealth v. Proetto*, 771 A.2d 823 (2001) in which U.S. law enforcement officials posed as a 15-year-old girl in a chat room. The suspect made sexually suggestive comments to the "underage female", which the U.S. law enforcement officials logged. The U.S. court reasoned that because the suspect communicated freely with the undercover agent and could not verify the law enforcement's official identity, he had no reasonable expectation of privacy in the chat communications. See also U.S. Court of Appeals for the Armed Forces, 21 November 1996, *United States v. Maxwell*, no. 95-0751 (1996) in which the U.S. court decided the suspect had no reasonable expectation of privacy in e-mail communications with an undercover U.S. law enforcement official, U.S. Court of Appeals of Ohio 6 February 2004, *Ohio v. Turner*, App. 3d 177 (2004), in which the court held that the suspect has no reasonable expectation of privacy in a chat room conversation with an undercover U.S. law enforcement official posing as an underage boy, and U.S. United States Court of Appeals (5th Circuit) 17 February 2010, *U.S. v. Underwood*, no. 08-31243 (2010), in which the U.S. law enforcement officer created an undercover profile purporting to be a 13-year-old boy and sent a friend request to the defendant. The defendant engaged the undercover officer in communication on the MySpace and Yahoo! Web sites, with much of the conversation having a sexual nature.

The prohibition of entrapment was developed in case law that applies to law enforcement officials who use undercover investigative methods. In brief, the U.S. entrapment doctrine dictates that U.S. law enforcement officials are not allowed "to induce an individual to commit an offense, who was otherwise not personally disposed to commit the offense".[115] Kerr explains that the 'inducement of a crime' occurs when an undercover agent pressures a suspect to commit an offence, by either badgering or encouraging him commit the offence in a calculated manner that is based on the suspect's personality (Kerr 2009, p. 591).[116] The suspect's predisposition to committing crimes (called the subjective test) is the most important factor in deciding whether some was pressured into committing a crime.[117] The behaviours of undercover agents are therefore to a (much) lesser extent decisive in determining whether entrapment has taken place (see Joh 2009, p. 172). Joh also observes that: "*the doctrine has not prompted courts to devise a 'meaningful definition of what constitute(s) impermissible participation in the offense' by the police. Most instances of police participation will not constitute entrapment so long as the defendant was a ready and willing criminal.*" In other words, the United States has adopted an entrapment test that differs significantly from the test used in the Netherlands, which also takes the active role of law enforcement officials explicitly into consideration (cf. Kruisbergen & De Jong 2010, p. 116). As a result, undercover law enforcement officials in the United States may, for example, sell illegal goods and then arrest individuals who were predisposed and bought them (Kruisbergen & De Jong 2010, p. 116). This undercover investigative method is not allowed in the Netherlands.[118]

B.2 Guidelines for U.S. law enforcement authorities

In the United States, undercover investigative methods are restricted by internal guidelines for law enforcement authorities. The Guideline for FBI Undercover Operations is briefly examined below, as it provides information with regard to the scope of the investigative methods and the manner in which they are applied in practice.[119]

In the United States, undercover investigative methods are not distinguished and regulated in a similar manner as in the Netherlands. For example, the regulations do not specify when undercover interactions with individuals undertaken by law enforcement officials are applied systematically and thus require special permission (cf. Kruisbergen & De Jong 2010, p. 112).

115 U.S. Supreme Court, *United States v. Russell*, 24 April 1973, 411, at 436 (1972).

116 With reference to U.S. 1st Circuit Court, *United States v. Gendron*, 28 February 1994, 955, at 961-962 (1994).

117 See U.S. Supreme Court, *Sorells v. The United States*, 19 December 1932, 287 U.S. 435 (1932), 356 U.S. Supreme Court, *Sherman v. United States*, 19 May 1958, 356 U.S. 369 (1958) and U.S. Supreme Court *Jacobson v. United States*, 6 April 1992, 503 U.S. 550 (1992).

118 See also explicitly section 2.8 under 'pseudo-selling' in the Guideline for Special Investigative Powers.

119 See the Attorney General's Guidelines on FBI Undercover Operations of 2002.

In the United States, undercover investigative methods are not restricted to particular crimes and do not require approval from a public prosecutor (cf. Ross 2007, p. 562). However, the aforementioned guidelines indicate that permission to conduct an undercover operation must be obtained from a 'Special Agent in Charge' at a local FBI office.[120] The request must detail why the proposed investigation will be effective and that it will be conducted in a minimally intrusive way. The Special Agent in Charge can then authorise undercover FBI agents to participate in certain offences, such as paying bribes, laundering money, and making controlled drug deliveries (so long as these deliveries do not enter the market) (Joh 2009, p. 177). Participation in more serious crimes requires advance approval from FBI headquarters (see Ross 2004, p. 587).[121] Undercover agents are only allowed to commit crimes (1) when necessary to obtain evidence that is not 'otherwise reasonably available', (2) to establish or maintain cover, or (3) to prevent serious bodily injury.[122] The guideline prescribes that "all reasonable steps must be taken to minimize the participation by FBI agents in illegal activity".[123] As explained in subsection 9.2.3, the appendix about 'On-line investigations' by FBI agents is classified. However, other local guidelines also indicate that authorisation is required for U.S. law enforcement officials to interact with individuals on the Internet in an undercover capacity and that 'authorisation levels' are comparable to other undercover investigative-activities in the physical world (cf. Global Information Sharing Initiative 2013, p. 14).[124]

C Notable differences

The Netherlands and the United States have fundamentally different approaches with regard to regulation of undercover investigative methods. In the Netherlands, most undercover investigative methods are regarded as privacy intrusive investigative methods that pose risks with regard to the integrity of criminal investigations. For that reason, certain undercover investigative methods are regulated in specific provisions in criminal procedural law. In the United States, however, undercover investigative methods are not seen as interfering with the privacy of individuals (cf. Kruisbergen et

120 See the Attorney General's Guidelines on FBI Undercover Operations of 2002, p. 4.

121 Joh (2009, p. 177) explains that when sensitive circumstances exist, such as when public officials or media organisations are targeted by an undercover operation, an undercover review committee must approve the operation. That committee consists of officials from the U.S. Department of Justice and the FBI.

122 See Attorney General's Guidelines on FBI Undercover Operations of 2002, p. 12.

123 See Attorney General's Guidelines on FBI Undercover Operations of 2002, p. 12.

124 See specifically the guideline of the U.S. Georgia Bureau of Investigation Investigative Division which states that agents can be authorised using an online alias to interact with a person on social media, when there is reason to believe that criminal offences have been, will be, or are being committed. The example is then provided of *"internet chat rooms where child exploitation occurs"*. The request must mention: (1) which online alias is used, (2) which social media accounts are utilised, (3) the valid law enforcement purpose, and (4) the anticipated duration for the undercover activity (see Global Information Sharing Initiative 2013, p. 32).

al. 2011, p. 398 and Ross 2007, p. 512). Undercover investigative methods are only restricted in internal guidelines, which regulations may vary between local and federal U.S. law enforcement authorities. Individuals involved in U.S. undercover operations cannot derive any rights from these guidelines.

The prohibition of entrapment forbids law enforcement officials in both States from enticing an individual to commit an offence that he did not intend to commit. However, the United States relies more heavily on the subjective test, which means that a suspect's predisposition to committing a crime is particularly important for determining whether entrapment has occurred. In the Netherlands, the active role of law enforcement officials in enticing an individual to commit an offence is also important for determining possible entrapment. As a consequence, U.S. law enforcement officials can play a more active role in undercover operations. For example, U.S. law enforcement authorities have extensive experience in posing as a minor in online chat rooms in child abuse investigations, whereas the legitimacy of this kind of undercover operations is debatable in the Netherlands.

In terms of legal certainty, these results mean that individuals should be aware that very different regulations apply to undercover investigative methods in the Netherlands and the United States. Dutch citizens will find it difficult to understand U.S. regulations for undercover investigative methods given the different notion of the right to privacy, the lack of statutory law for undercover investigative methods, and the different approach to entrapment under U.S. law.

9.4.3 Section conclusion

The analysis in subsection 9.4.1 has shown that cross-border unilateral online undercover investigations can produce extraterritorial effects when the individuals involved in the investigation are on foreign territory. The legal comparison between the Netherlands and the United States has shown that these States have a different view on the interference with territorial sovereignty that occurs when extraterritorial undercover investigations take place on foreign territory. Historically, U.S. law enforcement authorities have been more willing to conduct extraterritorial investigations using undercover investigative methods than their Dutch counterparts. It is too early to tell whether U.S. law enforcement authorities are still engaging in cross-border unilateral undercover operations, but then in an online context. However, the examined case of David Schrooten indicates that U.S. law enforcement officials have conducted evidence-gathering activities on Dutch territory without (prior) approval and have applied U.S. law to a Dutch citizen.

The willingness of U.S. law enforcement authorities to engage in cross-border unilateral undercover investigative activities can perhaps be explained in part by their different perspective on the right to privacy and undercover investigative methods. In the United States, undercover investigative methods are not considered to be privacy infringing and are not sub-

jected to statutory regulations. In contrast, the use of undercover investigative methods is regarded as a privacy intrusive evidence-gathering activity in the Netherlands.[125] From a Dutch perspective, a foreign law enforcement official's application of domestic regulations on a Dutch citizen without permission or an authorising treaty basis is regarded as a violation of Dutch sovereignty.

However, when the identity and location of the individual involved in an online undercover operation cannot be reasonably determined, it may be more acceptable to apply the investigative method unilaterally and across State borders. In this situation, the extraterritorial effects of the investigative method cannot be reasonably determined. When this exception is accepted, the question remains to which extent law enforcement officials must make efforts to identify and determine the location of the individual involved during the online undercover operation.

9.5 Hacking as an investigative method

This section examines the consequences of the cross-border unilateral application of hacking as an investigative method. Section 9.5.1 explores how the Netherlands and the United States each view the desirable restrictions for the cross-border unilateral application of this investigative method. Section 9.5.2 then compares how the two States regulate the method to identify the regulatory differences that illustrate the dangers to legal certainty. Finally, a section conclusion is provided in subsection 9.5.3.

9.5.1 Interferences with territorial sovereignty

The Netherlands and the United States agree that as part of territorial sovereignty, States themselves regulate under which circumstances law enforcement officials can search computers that are located on their territory.[126] When law enforcement officials conduct a search remotely on a computer that is located in another State, the territorial sovereignty of the affected

125 Of course, State power may also be a factor in the sense that other States may be reluctant to engage in extraterritorial evidence-gathering activities on U.S. territory, because the sanctions imposed by the United States for such a practice may have serious consequences for the State involved. It is difficult to estimate whether that is indeed a realistic scenario.

126 With regard to Dutch legislative history, see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (explanatory memorandum Computer Crime Act I), p. 11-12, *Kamerstukken II* (Parliamentary Series Second Chamber) 2004/05, 26 671, no. 10, p. 13. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 48. In the United States, the manual for securing electronic evidence developed by the U.S. Department of Justice warns that: *"in the event that U.S. law enforcement authorities inadvertently access a computer located in another State, appropriate government authorities should be consulted immediately" because "issues such as sovereignty may be implicated"* (DoJ Manual 2009, p. 58).

State may be infringed if no permission has been obtained and no authorising treaty basis is available.[127]

The extraterritorial effects of remotely accessing a computer are localised based on where the data that is stored within a computer system (cf. Koops & Goodwin 2014, p. 61). In order words, a 'computer-orientated jurisdiction principle' is used to localise the effects of hacking as an investigative method. In their extensive analysis regarding the applicable law to 'transborder access to computer systems', i.e., remote access to computers located anywhere without permission of the affected State or the use of legal assistance mechanisms, Koops and Goodwin (2014, p. 61) summarise the current view in international law as follows:

"the most solid view on what international law permits is that accessing data that are, or later turn out to be, stored on a server located in the territory of another state constitutes a breach of the territorial integrity of that state and thus constitutes a wrongful act (...) except where sovereign consent has been formally given".

However, this 'solid view in international law' frustrates law enforcement authorities. When the territorial restriction of enforcement jurisdiction is strictly interpreted and international law is fully respected, law enforcement officials cannot gain access to computer systems on foreign territory. No treaty basis that allows States to gain transborder access to computers is available. The Convention on Cybercrime only allows for this practice in very limited circumstances, namely when the data is publicly available to anyone or permission is obtained from the individual who has rightful access to that information (i.e., the suspect).[128]

The territorial restriction of enforcement jurisdiction in the context of hacking as an investigative method can lead to situation in which law enforcement officials are not able to gather evidence related to an individual who is located in their own State, because an individual uses an online service provider that stores or processes data on foreign territory. For example, Dutch law enforcement officials cannot access an interconnecting computer during a network search when that computer is located on foreign territory.[129] This interpretation severely restricts their possibilities for using network searches to gather evidence from interconnecting computers, since many online services make use of cloud computing and distribute their storage and processing activities among data centres all over the world. Dutch law enforcement officials would then have to assume that the data is likely

127 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (explanatory memorandum Computer Crime Act I), p. 11.

128 See art. 32(a)(b) of the Convention on Cybercrime.

129 See *Kamerstukken II* (Parliamentary Series Second Chamber) 2004/05, 26 671, no. 10, p. 13. An exception applies, for the situation that Dutch law enforcement officials can reasonably assume that the data is located in the Netherlands (*Kamerstukken II* (Parliamentary Series Second Chamber) 2004/05, 26 671, no. 10, p. 23).

stored or processed outside Dutch territory and cannot be obtained (see Koops et al. 2012b, p. 36). This assumption would in turn prevent Dutch law enforcement officials from using a network search to gain access to online services, such as webmail and online storage services.[130]

In my view, the following question should be addressed: Is the territorial sovereignty of the United States violated if Dutch law enforcement officials can access data related to a Dutch citizen who utilises a U.S. online service provider? That data is not necessarily located in the United States. In my view, cross-border unilateral network searches and remote searches should be possible when the following three requirements are met: (1) the individual who is involved in the criminal investigation is located in the investigating State, (2) law enforcement officials already possess the login credentials necessary to access the servers (hosting the content in the online account), and (3) a warrant to perform the search has been obtained from an investigative judge (Conings & Oerlemans 2013, p. 29-30).[131] In this situation, the interference with territorial sovereignty that occurs is not severe, since it is unclear where the interference takes place and which State is affected (cf. Koops & Goodwin 2014, p. 76 and Conings 2014, p. 14). In addition, the legal certainty of the individual involved is not endangered, because the cross-border unilateral access is conducted from a computer on the territory of the investigating State (where that individual is located).

In addition, when criminals utilise a system such as Tor, the network they use to access the Internet is obscured. Are law enforcement authorities then no longer allowed to remotely access a computer system under their own jurisdiction, because the computer that is accessed *might* be located on foreign territory? Similarly, when a criminal utilises anonymising services, such as proxy services and VPN services, it may not be possible to identify the computer user.[132] The use of anonymising services and cloud computing services have prompted the Dutch legislature and U.S. law enforcement authorities to propose an exception to the territorial limitation of enforcement jurisdiction, in order to allow for the cross-border unilateral application of hacking as an investigative method in special circumstances. These proposals are briefly examined below.

A The Dutch proposal

In its explanatory memorandum attached to the Computer Crime Act III, the Dutch legislature took a bold position with regard to the cross-border unilateral application of hacking as an investigative method. That memoran-

130 See the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53. See also subsection 8.2.1.

131 For instance, law enforcement officials can obtain these login credentials from a seized computer. They can then be used to gain access to the online account(s) of a suspect.

132 For instance, because the proxy service provider or VPN provider is located in a State that does not cooperate with law enforcement authorities of the investigating State, or because these providers did not log subscriber data and traffic data that is necessary to identify internet users.

dum states that "*when the location of the data cannot be reasonably determined*", remote access to that data is authorised.[133] As explained in the memorandum, this situation arises when suspects utilise services that enable cloud computing or anonymising services or techniques.[134] When the location of the data that is stored on computers is known, then permission of the State that will be affected by the investigative method is required or mutual legal assistance must be requested.[135] The main reason for this position is that the Dutch legislature wants to prevent the Internet from becoming a 'free haven' for criminals, which leads it to viewing certain forms of unilateral action as simply necessary (and apparently acceptable).[136]

The Computer Crime Act III proposes a new special investigative power that would enable Dutch law enforcement officials to remotely access a computer and then conduct a remote search and use policeware.[137] The proposal specifies that these officials would need to take the following factors into consideration when determining whether cross-border unilateral action is allowed:

(1) the seriousness of the crime;
(2) the degree of the involvement of the Netherlands (either by Dutch victims or the use IT infrastructure located in the Netherlands);
(3) the nature of the investigative techniques (e.g., remotely disabling data is deemed more intrusive than remote copying); and
(4) the risks for the integrity of the computers involved.[138]

These factors can indeed aid in interpreting the proportionality and subsidiary test that Dutch law requires be used when special investigative powers are applied. In my view, what is clearly missing from the explanatory memorandum is an understanding of the sensitivity and possible political repercussions of investigative activities that take place on foreign territory. Hacking as an investigative method is very intrusive investigative method. It is more likely that States will object when this investigative method is applied to a computer located on their territory than when other investigative methods are used, such as an online undercover investigation that only involves interaction with other individuals. In addition, unilateral hacking as an investigative method will make other States feel entitled to take recip-

133 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 51.
134 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 52.
135 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 46-47.
136 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 51
137 See also section 2.4 of chapter 8. The proposal also includes other types of hacking as an investigative method, but these are not examined in this study.
138 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 52

rocal actions in the form of using hacking as an investigative method from their own territory (cf. Koops & Goodwin 2014, p. 77 and AIV report 2014, p. 61). This aspect should also be explicitly taken into consideration when a decision is made to (allow for) remote access to a computer to gather evidence.

B The U.S. proposal

In the United States, U.S. criminal procedural law regulates the conditions under which a search warrant can be obtained to search a computer. In particular, Rule 41 of the U.S. Federal Rules of Criminal Procedure dictates the conditions for obtaining warrants to conduct searches, including remote searches. In brief, a 'Rule 41 search warrant' mirrors the requirements of the Fourth Amendment but adds extra requirements. The relevant rule dictates that a magistrate judge can issue a warrant at the request of a federal law enforcement officer or an attorney to search a place and 'seize particularly described things' (including digital information) in order to find evidence or contraband, when probable cause exists that the evidence or contraband is to be found at that place. The warrant can authorise governmental officials to seize 'electronic storage media' or 'seize or copy electronically stored information' in computers.

The text of Rule 41 currently restricts the warrant to "*the district of the court of the magistrate judge*". This restriction significantly limits the possibilities to conduct a remote search or install policeware in computers, since these investigative methods can only be applied within the district of the court of the judge.[139] The U.S. Department of Justice therefore seeks to amend Rule 41 to enable 'remote access' to computers and thus facilitate hacking as an investigative method. Its proposal is to amend Rule 41 so that its text holds that *"a magistrate judge with authority in any district where activities related to a crime may have occurred, has the authority to issue a warrant to use remote access to search electronic storage and to seize or copy electronically stored information located within or outside that district"*.[140]

With this proposal, the U.S. Department of Justice seeks to make remote searches possible in the following three situations: (1) when the district where the media or information is located has been concealed through technological means (e.g., by using anonymising software such as Tor), (2) when the victimised computers are located in five or more U.S. judicial districts (which typically applies when botnets are involved in cybercrimes), and (3) in the search of information that is accessible from a computer but is stored remotely in another district (e.g., remotely accessible cloud-based services

139 See Rule 41(b)(1): *"a magistrate judge with authority in the district-or if none is reasonably available, a judge of a state court of record in the district-has authority to issue a warrant to search for and seize a person or property located within the district"*.

140 The proposed amendment is available at: http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Standing/ST2014-05.pdf (last visited on 30 December 2014). See p. 499 and 500 and p. 600. Emphasis added by the author.

or web-based e-mail of an individual) (cf. Schwerha IV 2015, p. 2-3).[141] The U.S. Supreme Court used a special procedure to accept these changes in April 2016. The proposal was subsequently forwarded to the U.S. Congress, which now has until 1 December 2016 to halt or accept the amendment.[142]

Comparison of the proposals

The Dutch legislature and the U.S. Department of Justice have thus both proposed to allow hacking as an investigative method in similar situations. Simply stated, cross-border unilateral hacking as an investigative method is deemed permissible when the individuals involved in the criminal investigation utilise services that enable cloud computing or utilise anonymising services or techniques.

These approaches can be regarded as an exception to the generally accepted interpretation of the territorial restriction of enforcement jurisdiction that States cannot access computers on foreign territory without permission from the affected State or a treaty basis. Goldsmith (2001, p. 117-118) submits that certain applications of hacking as an investigative method with extraterritorial effects may even become customary among States.[143] I expect that law enforcement authorities all over the world will increasingly use hacking as an investigative method. As illustrated in this subsection, States can deem the cross-border unilateral application of hacking as an investigative method as necessary to overcome the obstacles of anonymity, encryption, and jurisdiction in cybercrime investigations. However, it is also conceivable that certain law enforcement authorities will apply the investigative method simply because it is a convenient way to gather evidence. The conditions under which cross-border unilateral hacking as an investigative method is ultimately accepted among States will depend on domestic legislation in individual States and responses within the international community.

141 See also p. 499 and 500 of the proposed amendment to Rule 41.

142 See, e.g., Danny Yadron, 'Supreme court grants FBI massive expansion of powers to hack computers', *The Guardian*, 29 April 2016. Available at: https://www.theguardian.com/technology/2016/apr/29/fbi-hacking-computers-warrants-supreme-court-congress (last visited on 25 May 2016).

143 Goldsmith argued that cross-border unilateral remote searches should not be regarded as an infringement of another State's sovereignty, but instead as part of *"the inevitably messy process of working out new customary principles of sovereignty to accommodate a new and important, but also potentially dangerous, technology"* (Goldsmith 2001, p. 117-118). Of course, at the same time, it should be pointed that States can only object to a practice when States are aware of the application of hacking as an investigative method and States claim responsibility for it.

9.5.2 Dangers to legal certainty

Hacking as investigative method is a particularly intrusive investigative method that seriously interferes in the rights and freedoms of the individuals involved. When foreign law enforcement officials gain remote access to a computer of a citizen on foreign territory, that individual's legal certainty is endangered.

This subsection highlights the differences in the regulations for hacking as an investigative method using a brief comparison of the Dutch and U.S. situations. The Dutch legal framework for hacking as an investigative method has already been examined extensively in chapter 8. A summary of the results of that analysis is provided under A below. A brief analysis of the U.S. (federal) regulations for the investigative method is then conducted under B. Finally, the most important differences between Dutch and U.S. regulations are identified under C.

A Overview of Dutch regulations

Hacking as investigative method has been categorised as (1) network searches, (2) remote searches, and (3) the use of policeware. The analysis in chapter 8 has shown that in the last five years, the regulations and procedural safeguards that apply to regular powers for searching a place and seizing computers have been used as a legal basis for network searches and remote searches. Remote searches are considered as more privacy intrusive than network searches, since they can be applied covertly (whereas network searches must still be conducted during a search at a particular place). The use of policeware can be derived from the existing legal basis for recording private communications, which is also regulated as a special investigative power in Dutch law. However, in order to use all functionalities of policeware, i.e., those that go beyond the recording of private communications (such as taking screen shots), special provisions with appropriate procedural safeguards must be created. Using policeware is considered to be the most privacy intrusive investigative method examined in this study, given that it involves remote access to computer systems, is applied covertly, and enables law enforcement officials to both take specific functions of computers over and monitor an individual's computer behaviours.

The Dutch legislature now has to decide whether to accept the proposal for a new Computer Crime Act (i.e., Computer Crime Act III), which includes the special investigative power to 'gain remote access to computers' (i.e., to hack computers). The proposed special investigative power incorporates remote searches and the use of policeware, but excludes network searches that are already regulated in a separate investigative power in the DCCP. The proposal for a special investigative power for hacking as an investigative method details appropriate strong procedural safeguards.[144]

144 In chapter 8, concerns were raised with regard to the scope of the proposed special investigative power.

However, it was argued Dutch legislature should scrutinise the scope of the proposed special investigative power. It was also argued that the special investigative power for network searches should include a warrant requirement from an investigative judge.

B Overview of U.S. regulations for the investigative method

The U.S. regulations for hacking as an investigative method are first examined with regard to the method's relation to the Fourth Amendment to the U.S. Constitution. This analysis determines whether a warrant is required to apply this investigative method. The regulations in U.S. criminal procedural law (namely Rule 41 of the U.S. Federal Rules of Criminal Procedure) were already examined in subsection 9.5.1 and are not repeated here.[145]

Fourth Amendment to the U.S. Constitution

When U.S. law enforcement officials undertake domestic investigations, they most often have to obtain a warrant to apply hacking as investigative method as meant in this study. The distinguished types of hacking as an investigative method, i.e., (1) network searches, (2) remote searches, and (3) the use of policeware, can all be applied insofar as a warrant is obtained from a U.S. judge. More particularly, U.S. law enforcement officials typically need to acquire a Rule 41 warrant, as described in subsection 9.5.1.

A warrant is required because gaining remote access to a computer (the first step when performing hacking as an investigative method) can essentially be regarded as a 'search' when considered in the context of the Fourth Amendment to the U.S. Constitution. In the United States, computers are viewed as 'containers', analogous to letters, packages, boxes, and trunks (cf. Kerr 2010, p. 309). In this regard, the basic rule is that individuals have a reasonable expectation of privacy with regard to a container's contents. As a result, the Fourth Amendment warrant requirement generally applies to the seizure of computers and subsequent search and seizure of the data within them (cf. Kerr 2010, p. 309).[146]

However, whether the Fourth Amendment also protects the seizure of computers and subsequent search and seizure of their data that takes place directly after an arrest was debated until 2014.[147] This so-called 'search incident to arrest' exception to the warrant requirement enabled law enforcement officials to seize a computer within a reasonable time following an arrest without having to obtain a warrant from a U.S. judge.

---

145 The manual for Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations of the U.S. Department of Justice (DoJ Manual 2009) is also referred to when it provides additional relevant information. The manual does not refer to the use of remote searches or policeware as investigative methods. However, it does indicate that a warrant is required for a network search (see DoJ Manual 2009, p. 84).

146 In the United States, exceptions for searching computers at national borders (e.g., at airports) apply. These exceptions are not further examined in this study.

147 See, e.g., Brenner 2011 and Gershowitz 2008.

In the landmark 2014 case of *California v. Riley*, the U.S. Supreme Court decided that a warrant is required to seize a cell phone immediately following an arrest.[148] Due to this decision, the 'search incident to arrest' exception no longer applies in the United States. The U.S. Supreme Court asserted that today's cell phones should not be treated as regular objects. This view is reflected in the *Riley* decision as follows:

"Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life," (...). The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant."[149]

The facts that cell phones are no longer regarded as regular objects and law enforcement offices must obtain warrants to seize and subsequently search and seize their contents also leads to the conclusion that the warrant requirement also applies to other computers. A (Rule 41) warrant is therefore also required to perform a network search (cf. DoJ Manual 2009, p. 84-85) or remote search (cf. Brenner 2012).

From case law, it is also clear that U.S. law enforcement officials must obtain a Rule 41 warrant to utilise policeware.[150] In a 2013 judgement, a U.S. judge denied a warrant request for using policeware. The request stipulated that that warrant was needed to enable federal law enforcement officials to:

"surreptitiously install data extraction software on the Target Computer. Once installed, the software has the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within the district."[151]

The case thus confirms that U.S. law enforcement authorities require a (Rule 41) warrant to use policeware. The description of the functionalities of the policeware also indicate the scope of the investigative method.

148 U.S. Supreme Court, 25 June 2014, *Riley v. California*, 573 U.S. (2014).

149 U.S. Supreme Court, 25 June 2014, *Riley v. California*, 573 U.S., at 32 (2014).

150 However, data access requests have revealed that U.S. law enforcement officials remotely installed and used policeware as early as 2007. See Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', *Wired*, 18 July 2007. Available at: http://archive.wired.com/politics/law/news/2007/07/fbi_spyware (last visited on 30 December 2014).

151 See Cyrus Farivar, 'FBI denied permission to spy on hacker through his webcam', *Ars Technica,* 25 April 2013. Available at: http://arstechnica.com/tech-policy/2013/04/fbi-denied-permission-to-spy-on-hacker-through-his-webcam/ (last visited on 30 December 2014).

The U.S. judge denied the warrant request in the above case, on the basis that the Rule 41 requirements (including the territorial limitation of the warrant) were not satisfied.[152] With regard to the dangers to legal certainty, the following statement of the judge is relevant:

"*That search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name*".[153]

This statement eloquently indicates how individuals can be subjected to U.S. governmental power when a warrant is issued to install policeware on a computer with an unknown location. As foreign laws cannot be accessible or foreseeable to individuals, those individuals involved are subjected to arbitrary governmental interference in their private lives.

In summary, U.S. law enforcement authorities in principle require a (Rule 41) warrant to (1) perform a network search, (2) perform a remote search, or (3) make use of policeware. However, an important exception has been formulated in relation to 'computer searches on foreign territory'. This exception is further examined below.

No warrant required for computers outside U.S. territory?

In the landmark case of *United States v. Verdugo-Urquidez*, the doctrine was established that only U.S. citizens and individuals located on U.S. territory are protected by the U.S. Constitution.[154] Following the decision, U.S. law enforcement officials do not require a warrant to search a place of a non-U.S. individual outside U.S. territory. The case is briefly examined below.

The case of *United States v. Verdugo-Urquidez* involved a criminal investigation with regard to drug trafficking and the murder of a U.S DEA agent. In this case, U.S. DEA law enforcement officials worked together with local Mexican authorities. The U.S. law enforcement authorities searched a residence located on Mexican territory without a U.S. warrant. However, the local Mexican law enforcement authorities reportedly authorised the U.S. law enforcement officials to perform the search. The U.S. law enforcement officials found records of marijuana shipments made by the suspect inside the residence, who was subsequently brought to the United States for trial. When the suspect protested that U.S. law enforcement authorities were supposed to obtain a warrant to search his residence in Mexico, the U.S

152 See subsection 9.5.1.

153 See U.S. District Court Southern District of Texas Houston Division, *In Re Warrant To Search a Target Computer at Premises Unknown*, 22 April 2013, 958 F.Supp.2d 753.

154 U.S. Supreme Court 28 February 1990, *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

Supreme Court decided that U.S. law enforcement officials do not require a warrant to search the residence of a non-U.S. citizen on foreign territory.[155]

As a result of the *United States v. Verdugo-Urquidez* case, U.S. law enforcement officials who undertake search and seizures measures as outside U.S. territory in situations that do not involve a U.S. citizen do not require a warrant under the Fourth Amendment to the U.S. Constitution (cf. Gane & Mackarel 1996, p. 109, Vander Beken 1999, p. 249). Milanovic (2015, p. 89) describes the doctrine as a manifestation of the idea of a social contract, namely that privacy protections are only awarded to citizens or individuals living on the territory of the investigating State. This doctrine may have consequences for the warrant requirement for using hacking as an investigative method. Two hacking cases that have referred to this doctrine are briefly examined below.

In the case of *United States v. Gorshkov*, FBI officials lured two Russian suspects to the United States for job interviews at the fake IT security company 'Invita' in 2001.[156] During their interviews, the individuals were requested to demonstrate their computer skills by hacking into a network that had been set up by the FBI. The suspects consequently downloaded hacking tools from the website 'tech.net.ru', which was located on their own servers in Russia. The FBI agents had installed a keylogger on the laptop they provided to the Russian suspects, which enabled them to subsequently record the login credentials that the suspects used to gain access to two servers located on Russian territory. The U.S. Department of Justice reportedly requested legal assistance from Russian authorities to obtain the data from the Russian servers, but they did not receive a reply. After several unsuccessful attempts to convince the Russian authorities to co-operate, the FBI used the collected usernames and passwords to access the two servers and subsequently download a total of 1.3 gigabytes of information from them.[157] During the trial, it became apparent that the FBI agents had downloaded the files from the Russian server without a warrant (which was obtained later in

155 U.S. Supreme Court 28 February 1990, *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). However, see also Judge Brennan's dissenting opinion at 283-284, stating that: *"What the majority ignores, however, is the most obvious connection between Verdugo-Urquidez and the United States: he was investigated and is being prosecuted for violations of United States law and may well spend the rest of his life in a United States prison. The 'sufficient connection' is supplied not by Verdugo-Urquidez, but by the Government. Respondent is entitled to the protections of the Fourth Amendment because our Government, by investigating him and attempting to hold him accountable under United States criminal laws, has treated him as a member of our community for purposes of enforcing our laws. He has become, quite literally, one of the governed."*

156 See U.S. District Court of Washington, *United States v. Gorshkov*, 23 May 2001, F.Supp.2d, 2001 WL 1024026, 23 May 2001, at 1.

157 Robert Lemos, 'FBI "hack" raises global security concerns', *CNET News*, 1 May 2001. Available at: http://news.cnet.com/FBI-hack-raises-global-security-concerns/2100-1001_3-256811.html (last visited on 30 July 2015).

time) and used the collected data as trial evidence.[158] In response, the Russian Federal Security Service charged one of the involved FBI agents with computer hacking on Russian territory in 2002.[159]

At trial, the Russian suspects objected to the evidence-gathering activity, arguing that they were protected by the Fourth Amendment to the U.S. Constitution, which requires law enforcement officials to have a warrant to conduct a search. With regard to whether a warrant was required, the judge decided that:

"The Fourth Amendment does not apply to the agents' extraterritorial access to computers in Russia and their copying of data contained thereon. First, the Russian computers are not protected by the Fourth Amendment because they are property of a non-resident and located outside the territory of the United States. Under United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), the Fourth Amendment does not apply to a search or seizure of a non-resident alien's property outside the territory of the United States. In this case, the computers accessed by the agents were located in Russia, as was the data contained on those computers that the agents copied. Until the copied data was transmitted to the United States, it was outside the territory of this country and not subject to the protections of the Fourth Amendment"[160]

The judge thus decided that suspects were therefore not protected by the Fourth Amendment. The judge also found that Russian law did not apply either.[161] Their legal position can thus be described as a 'legal vacuum'.

In the case of *United States v. Ross Ulbricht*, a U.S. prosecutor also argued that a warrant is not required to search a computer that is located on foreign territory and belongs to a foreign company (e.g., a hosting provider).[162] The prosecutor's argument was as follows:

158 The data reportedly provided a 'wealth of evidence'. The databases contained more than 56,000 credit cards, bank account information, and other personal information of individuals. See U.S. Department of Justice Press Release, 'Russian Computer Hacker Convicted by Jury', 10 October 2002. Available at: http://www.justice.gov/criminal/cybercrime/press-releases/2001/gorshkovconvict.htm (last visited on 30 July 2015).

159 John Leyden, 'Russians accuse FBI agent of hacking', *The Register*, 16 August 2002. Available at: http://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/ (last visited on 30 July 2015).

160 U.S. District Court of Washington, *United States v. Gorshkov*, 23 May 2001, F.Supp.2d, 2001 WL 1024026, 23 May 2001, at 3. Emphasis added.

161 U.S. District Court of Washington, *United States v. Gorshkov*, 23 May 2001, F.Supp.2d, 2001 WL 1024026, 23 May 2001, at 4: "*As to Defendant's contention that the FBI's actions were unreasonable and illegal because they failed to comply with Russian law, the Court finds that Russian law does not apply to the agents' actions in this case and even if it were to apply, the agents sufficiently complied with the relevant portions of the Criminal Process Code of Russia.*"

162 See subsection 2.3.3 for a more extensive analysis of the Silk Road investigation.

Because the [Silk Road] server was located outside the United States, the Fourth Amendment would not have required a warrant to search the server, whether for its IP address or otherwise (…). Given that the SR server was hosting a blatantly criminal website, it would have been reasonable for the FBI to "hack" in to it in order to search it, as any such "hack" would simply have constituted a search of foreign property known to contain criminal evidence, for which a warrant is not necessary".[163]

The U.S. law enforcement officials never confirmed that they obtained remote access to the server of the Silk Road forum.[164] The contents of the server were eventually acquired using a mutual legal assistance request from law enforcement authorities in Iceland.

However, Brenner and Kerr argue that a warrant is still required when U.S. law enforcement officials remotely access computers on foreign territory, because that investigating activity *also* takes place on U.S. territory as part of a domestic criminal investigation.[165] Indeed, a key characteristic of cross-border unilateral digital investigative activities is that they occur on territory of both the investigating State and another State simultaneously (cf. Forcese 2011). To deny the safeguards that criminal procedural law offers based solely on the fact that the individuals involved are on foreign territory makes no sense (cf. Van der Wilt 2000, p. 186).[166] When neither local nor foreign laws are applied, these individuals are placed in a legal vacuum and deprived of protection from either legal system. It appears that the proposed amendment to the Rule 41 warrant will always require a warrant for U.S. law enforcement officials who want to use hacking as an investigative method.

---

163 See the government response to the declaration of Joshua Horowitz in *United States v. Ross Ulbricht*, S1 14 Cr. 68 (KBF), p. 7. With regard to the facts of the *Silk Road* investigation, see, e.g. Nate Anderson and Cyrus Farivar, 'How the feds took down the Dread Pirate Roberts', *Ars Technica,* 3 October 2013. Available at: http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/, Kim Zetter, 'How the Feds Took Down the Silk Road Drug Wonderland', 18 November 2015. Available at: http://www.wired.com/2013/11/silk-road/, and Joshuah Bearman, 'Silk Road: The Untold Story', *Wired*, 23 May 2015. Available at: http://www.wired.com/2015/05/silk-road-untold-story/ (last visited on 30 September 2015).

164 See Andy Greenberg, 'Ross Ulbricht Calls For New Trial, Alleging Feds Hacked Tor', *Wired*, 9 March 2015. Available at: http://www.wired.com/2015/03/ross-ulbricht-calls-new-trial-alleging-feds-hacked-tor/ (last visited on 30 September 2015).

165 See S. Brenner, 'Our Fourth Amendment', 11 March 2006. Available at: http://cyb3r-crim3.blogspot.nl/2006/03/our-fourth-amendment.html and Orin Kerr, 'Fascinating New Case on Legal Standards for Searching a Remote Computer With Unknown Location', The Volokh Conspiracy (blog), 26 April 2013. Available at: http://volokh.com/2013/04/26/fascinating-new-case-on-legal-standards-for-searching-a-remote-computer-with-unknown-location/ (last visited on 25 January 2015).

166 See also the more articulate dissenting opinion of Judge Brennan in *Verdugo-Urquidez v. United States*, at 283-284: *"Fundamental fairness and the ideal underlying our Bill of Rights compel the conclusion that when we impose societal obligations such as the obligation to comply with our criminal laws, on foreign nationals, we in turn are obliged to respect certain correlative rights, among them the Fourth Amendment."*

C Notable differences

The Netherlands and the United States have different legal frameworks for hacking as an investigative method.

In the Netherlands, the legislature aims to create a new special investigative power for remote searches and the use of policeware in Dutch criminal procedural law. The proposal specifies that law enforcement officials require a warrant from an investigative judge to apply the investigative power. However, the legal basis for network searches is not amended and still mirrors the regulations for computer searches. In the Netherlands, no warrant is required for computer searches, unless the search and subsequent seizure of a computer takes place within a residence.

In the United States, a warrant is required for the identified types of hacking as an investigative method, insofar as a computer is located on U.S. territory or the computer belongs to a U.S. individual. Based on the *United States v. Verdugo-Urquidez* case, it can be argued that the Fourth Amendment only applies to U.S. citizens or computers on the territory of the United States. Kerr and Brenner have argued that the Rule 41 warrant is nevertheless applicable, since the investigation takes place on U.S. territory as well as on foreign territory. Which interpretation U.S. law enforcement authorities have adopted remains unclear.

From a Dutch perspective, the territorial limitation of the Fourth Amendment warrant requirement is peculiar. In the Netherlands, Dutch law also applies when evidence-gathering activities are applied on the territory of another State. In the context of the cross-border unilateral application of hacking as an investigative method, the U.S. territorial limitation of the Fourth Amendment is troubling from the perspective of legal certainty. It is possible that when this investigative method is applied unilaterally across State borders, neither U.S. law nor the domestic regulations of the State where that computer is located are applicable – which puts the citizen involved in a legal vacuum.

9.5.3 Section conclusion

Hacking is an intrusive investigative method that infringes on the territorial sovereignty of another State when the targeted computer is located on foreign territory. For that reason, law enforcement authorities are not allowed to gain remote access to computers that are located on foreign territory without permission from the affected State or a treaty basis that authorises the evidence-gathering activity.

However, the legislative bodies in both the Netherlands and the United States aim to allow cross-border unilateral hacking as an investigative method when, simply put, the location of the computer targeted for remote access is unclear, the search is proportionate considering the circumstances at hand, and no other alternatives for gathering the information are available. Law enforcement authorities in both countries clearly feel the need to deploy hacking techniques to combat cybercrime more effectively (cf. Brenner 2012, p. 91-92).

However, applying cross-border unilateral hacking as an investigative method will make other States feel entitled to take reciprocal actions in the form of applying this investigative method from their own territory (cf. Koops & Goodwin 2014, p. 77 and AIV report 2014, p. 61). It is difficult to foresee the reciprocal effects and thereby the consequences for citizens and companies that may arise were foreign law enforcement authorities to do so. The worst-case scenario would be a situation in which law enforcement authorities hack computers on the territory of other States under their own domestic regulations. In such a 'digital legal jungle' where many local regulations for investigative methods are applied extraterritorially by law enforcement authorities, a State's citizens would not know if law enforcement authorities have obtained (unauthorised) access to their computers and then conducted other investigative activities. They would also not be aware of the conditions for applying hacking as an investigative method in criminal investigations.

9.6 Restrictions for the identified investigative methods

This section examines the desirable restrictions for the cross-border unilateral application of the identified investigative methods. The proposals made are based on the analyses in the previous sections and focus on the evidence-gathering activities that are conducted by Dutch law enforcement officials. These proposals can be considered as a first step towards developing a policy for cross-border unilateral cybercrime investigations. The details of both the desirable procedures and the treaty provisions must be further examined and developed. It is important that all States start to include the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. They should also make an effort to reach agreements with other States as to the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable. The EU should also incorporate the concept of (cross-border unilateral) digital evidence-gathering activities within the EU legal framework for legal assistance. Finally, the Council of Europe should continue its efforts to include States in the Convention on Cybercrime and further develop regulations for 'cross-border access to computers'.

This section further focuses on the desirable restrictions of the cross-border unilateral application of the identified digital investigative methods for Dutch law enforcement authorities. The extent to which it is desirable to apply each identified investigative method unilaterally across State borders is examined separately in subsections 9.6.1 to 9.6.4.

9.6.1 Gathering publicly available online information

The analysis in section 9.2 has shown that gathering publicly available online information that is located on foreign territory likely does not infringe

the territorial sovereignty of other States. The reasons are that States tacitly allow for the cross-border unilateral gathering of this information and the potential infringement to the territorial sovereignty of States appears to be minor. Dutch law enforcement authorities are therefore allowed to gather publicly available online information both across State borders and unilaterally.

However, this practice may endanger the legal certainty of the individuals involved. For example, in the Netherlands, detailed regulations apply in relation to systematic observation of the online behaviours of individuals. When foreign law enforcement officials are allowed to systematically observe the behaviours of Dutch citizens, the domestic regulations for those foreign law enforcement authorities are not foreseeable to the individuals involved. It would be preferable from a fundamental rights perspective if the Netherlands could specify in treaties the conditions under which the systematic online observation of individuals is allowed. However, the extraterritorial gathering of publicly available online information, that typically includes information that can be obtained by observation, is already arguably international customary law. It is also problematic for States to detect the application of the investigative method, due to the nature of the Internet, which practically allow foreign law enforcement authorities to apply the investigative method anonymously, across borders, and in a unilateral manner. I am not convinced that States would be willing to conclude treaty agreements with regard to this evidence-gathering activity, given that their law enforcement officials are already applying it with little chance of repercussions for their actions.

9.6.2 Data production orders

The analysis in section 9.3 has shown that the cross-border unilateral issuance of data production orders to (foreign) online service providers may interfere with the territorial sovereignty of the State where the company is located and the States where the data is stored on computers. As part of their territorial sovereignty, States can decide under which circumstances companies can disclose data to foreign law enforcement authorities.

However, online service providers can provide their services to individuals located anywhere in the world. Online service providers make use of cloud computing, which make it difficult to pinpoint the location of the data and thereby difficult to determine where the extraterritorial effects of the investigative method takes place. A practice has arisen where certain (U.S.) online service providers voluntarily disclose non-content data to foreign law enforcement authorities when (in their eyes) valid data production orders are issued. To obtain content data, it appears that a U.S. warrant and mutual legal assistance is required. The practice of voluntarily disclosure is less burdensome than applying legal assistance mechanisms for law enforcement authorities. However, the voluntarily disclosure of information does endanger the legal certainty of the individuals involved.

Therefore, it is preferable that States negotiate a treaty that regulates unilateral data production orders that are issued to online service providers (cf. De Schepper & Verbruggen 2013, p. 166 and Verbruggen 2014, p. 140). Such a treaty should differentiate between different safeguards to obtain the identified categories of data from online service providers according to their sensitivity and thereby protect the individuals involved. It would be preferable for the Council of Europe to negotiate a provision in the Convention on Cybercrime or an extra protocol, seeing as many States have already ratified the Convention on Cybercrime.

In the past five years, working groups designated by the Council of Europe have been unable to propose amendments or a new protocol to the Convention on Cybercrime to regulate unilateral data production orders (cf. Koops & Goodwin 2014, p. 58). The urgency for regulation will only increase in the future, since the information available at online service providers that is relevant for law enforcement authorities will continue to grow. Alternatively, the EU could attempt to conclude a treaty with the United States that dictates the conditions under which law enforcement authorities can use data production orders to obtain the data of these providers' customers.[167]

9.6.3 Online undercover investigative methods

The analysis in section 9.4 has shown that undercover operations conducted by investigative officials during the course of criminal investigations produce extraterritorial effects that, without consent from or a treaty basis with the affected State, intrude on the territorial sovereignty of that State. For that reason, Dutch law enforcement officials are in theory not allowed to conduct undercover operations that involve individuals who are located on foreign territory (cf. Siemerink 2000a, p. 80). The analysis has also shown that States regulate (online) undercover investigative methods in different ways. In order to respect State sovereignty and the rights and freedoms of the individuals involved, it is recommended that Dutch law enforcement officials seek legal assistance or otherwise obtain permission when they know that an individual involved in an online undercover investigation is on foreign territory. The involvement of foreign law enforcement authorities is often required eventually anyway, given that further criminal procedural powers (such as for searching and seizing physical places and making arrests) will have to be applied by the local law enforcement authorities to successfully prosecute individuals who are located on foreign territory.

---

167 In this respect, the press release of the Council of the European Union on 9 June 2016, 'Fight against criminal activities in cyberspace: Council agrees on practical measures and next steps', in which the council concludes that action is required *"in the area of improving cooperation with service providers, through the development of a common framework (e.g. use of aligned forms and tools) with them to request specific categories of data"*. Available at: http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/ (last visited on 8 June 2016).

However, when the location of the individual involved is unknown, Dutch law enforcement officials should be able to apply cross-border unilateral online undercover investigations. The reason is that the extraterritorial effects of the investigative method cannot be reasonably determined and the legal regime in international law cannot be applied in such a situation. When an individual's location becomes apparent, the investigating law enforcement authorities should notify the relevant State and either obtain permission to continue the operations or initiate mutual legal procedures.

It would be preferable for States to agree on the above-mentioned procedure for online undercover investigative methods in new or existing mutual legal assistance treaties. However, similar to when systematic online observation is applied as an investigative method, it is questionable whether States would be willing to agree on the terms under which undercover systematic interactions with foreign individuals are allowed. It may be difficult for the affected State to detect – and object to – the practice of this undercover investigative method, given the method's limited intrusiveness in terms of intruding on sovereignty. At the same time, the case of David Schrooten illustrates how such an operation can ultimately lead to controversy and unrest in the affected State. States must also consider the reciprocal effects of the online undercover practices of their law enforcement authorities.

9.6.4 Hacking as an investigative method

The analysis in section 9.5 has shown that performing hacking as an investigative method on computers located on foreign territory interferes with the territorial sovereignty of the State where the targeted computer is located. Without permission from that State or an authorising basis in a treaty, the cross-border unilateral application of this investigative method is thus not allowed.

Legislative bodies in both the Netherlands and the United States aim to make the application of cross-border unilateral hacking as an investigative method possible when the location of the computer that is targeted for remote access is unclear. From a law enforcement perspective, the cross-border unilateral application of hacking as an investigative method in these circumstances is understandable, because the use of anonymising and cloud computing services frustrates the efforts of law enforcement officials to gather evidence in cybercrime investigations. I have argued that the Dutch legislature (so far) has failed to fully recognise the sensitivity and possible political repercussions of these investigative activities. Hacking as an investigative method is very intrusive, and States are more likely to object when it is applied to computers located on their territory than when other investigative methods are applied. Possible reciprocal applications of the method must also be explicitly taken into consideration by both law enforcement officials and the judiciary when a decision is made to remotely access a computer to gather evidence.

However, a proportionate application of hacking as an investigative method may be desirable when the location of the computer involved cannot be reasonably determined and a suspect makes use of cloud computing. An approach that may be less controversial is to allow cross-border unilateral network searches and remote searches when the following three requirements are met: (1) the individual who is involved in the criminal investigation is located in the investigating State, (2) law enforcement officials already possess the login credentials necessary to access the computers, and (3) a warrant to perform the search has been obtained from an investigative judge (Conings & Oerlemans 2013, p. 29-30).[168] The interference with territorial sovereignty that takes place is not severe, since it is unclear where the interference occurs and which State is affected (cf. Koops & Goodwin 2014, p. 76 and Conings 2014, p. 14). An advantage of this approach is also that the legal certainty of the individuals involved is not endangered when these types of searches are conducted, as cross-border unilateral access is achieved from a computer on the investigating State's territory (which is also where the individuals involved are located). The use of policeware as an investigative method should in my view be restricted to computers located on the investigating State's territory. When the location of the computer that is about to be 'infected' with policeware is unknown, law enforcement officials should restrict the software's functionalities to localising the computer that is used by the individual in question.

9.7 Chapter conclusion

The aim of this chapter was to determine the extent to which is it desirable that the identified investigative methods are applied unilaterally across State borders. To achieve that aim, the legal implications of cross-border unilateral digital investigations in terms of sovereignty and legal certainty have been examined (RQ 5). Three steps have been taken specifically to answer the research question. The first step entailed examining the consequences of a cross-border unilateral application of the identified investigative methods. In the second step, a legal comparison of the Netherlands and the United States was conducted to illustrate how each State views the desirable restrictions for the cross-border unilateral application of the investigative methods and actually regulates each method. Based on the outcomes of these two steps, the third step involved making proposals for desirable restrictions to a cross-border unilateral application of the investigative methods from a Dutch perspective. The results of these steps are summarised below.

168 For instance, law enforcement officials can obtain these login credentials from a seized computer and then use them to gain access to a suspect's online account(s).

Step 1 – Consequences of cross-border unilateral investigations
This first step was addressed in section 9.1. The cross-border unilateral application of investigative methods can have extraterritorial effects that lead to an interference of the *territorial sovereignty* of the State involved, insofar as permission is not obtained from that State or a treaty basis is unavailable for the evidence-gathering activity. States respond differently to these interferences, depending on the intrusiveness of the investigative method that is used and factors such as past grievances with other States.

As a corollary of the territorial limitation of enforcement jurisdiction that serves to protect State sovereignty, the individuals located in a State are protected against arbitrary interferences from *foreign* law enforcement authorities in their private lives. The cross-border unilateral application of investigative methods can therefore lead to a situation in which foreign laws are applied to individuals who are located in the affected State. The foreign regulations that restrict the application of investigative methods are not accessible and not foreseeable to the individuals involved and will endanger the *legal certainty* of the individuals involved. Other actors engaged in the criminal justice system also require legal certainty about the conditions under which digital evidence-gathering activities are applied.

Step 2 – Legal comparison between the Dutch and U.S. approaches
The legal comparison that was part of the second step was conducted in sections 9.2 to 9.5. The analysis emphasised the different interpretations of the Netherlands and the United States regarding the principle of the territorial limitation of enforcement jurisdiction. Most notably, the analysis shown that the United States has previously engaged in the unilateral application of extraterritorial undercover investigative methods and data production orders. This practice is now likely sustained in the application of these investigative methods in an online context. However, there is not sufficient information is available to fully indicate the extent to which U.S. law enforcement authorities apply these digital investigative methods unilaterally across State borders.

In contrast, the Netherlands follows a more careful approach when the application of investigative methods produces extraterritorial effects. The legal comparison showed that the Netherlands views the application of the identified digital investigative methods as privacy intrusive and has regulated many of them in statutory law. In the United States, only the issuing of data production orders and hacking as an investigative method are regulated in statutory law. The gathering of publicly available online information and online undercover investigative method are regulated in internal guidelines. Citizens cannot derive any rights from these guidelines and their contents may vary depending on the U.S. law enforcement authority that is involved. Considerably stricter regulations apply to these two investigative methods in the Netherlands. Interestingly, both Dutch and U.S. law enforcement officials have engaged in cross-border unilateral hacking as an investigative method. Legislative bodies in both States also aim to regulate

cross-border unilateral hacking as an investigative method in the event that the target computer cannot be reasonably localised.

Overall, it should be observed that a discrepancy between theory and practice appears to exist. In theory, extraterritorial evidence-gathering activities are not allowed without permission from the affected State or a treaty basis for the evidence-gathering activity. In practice, however, cross-border unilateral digital evidence-gathering activities can – and do – take place. It is crucial that the reality of cross-border unilateral evidence-gathering activities in cybercrime investigations is dealt with and that thinking is developed about desirable restrictions in this regard. All States should start including the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. States should also endeavour to reach agreements with other States as to the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable.

Step 3 – Proposal for desirable restrictions

The third step, which was undertaken in section 9.6, entailed making proposals to regulate Dutch law enforcement officials' cross-border unilateral application of the investigative methods based on the relevant consequences identified. An overview of the results of that analysis, indicating to which extent the cross-border unilateral evidence gathering may be acceptable and thus the answers RQ 5 is provided in Table 9.1.

Investigative method	**Should the cross-border unilateral evidence-gathering activity be possible?**	**Recommended action**
Gathering publicly available online information	Yes, based on art. 32(a) of the Convention on Cybercrime. The practice is arguably part of international customary law.	It is preferable to regulate the application of systematic online observation in a treaty.
Data production orders issued to online service providers	Yes, insofar as the online service provider voluntarily cooperates.	It is preferable to regulate the application of unilateral data production orders to online service providers in a treaty.
Online undercover investigative methods	(1) Yes, insofar as the individual involved is located in the investigating State. (2) Yes, insofar as the location of the individual involved is unknown and the investigating State notifies the other State and either obtains permission or initiates mutual legal assistance procedures, as soon as the involved individual's location does become known.	States should refrain from online undercover investigation activities when it is clear that the individual involved is located on foreign territory. It is preferable to regulate the application of online undercover investigations in a treaty.
Hacking as an investigative method	(1) Yes, insofar as (A) the remote and network searches involve the online accounts or computers of an individual who is located in the investigating State's territory, (B) law enforcement officials already possess the login credentials necessary to remotely access computers, and (C) a warrant to perform the search has been obtained from a judge. (2) No, insofar as the computer targeted for policeware is clearly located on foreign territory. When this is not clear, the use of policeware should be restricted to localising the computer.	States should continue negotiations in order to agree on the terms under which remote access to computer systems on foreign territory is allowed.

Table 9.1: Proposed restrictions and regulations for the cross-border unilateral application of the identified digital investigative methods.