Interception of electronic communications

The (dis)approval of backdoors in an increasingly encrypted digital world

Master Thesis Law & Technology

E.A.F. van Noort
SNR: 1258673

Tilburg University
10 May 2018
First Supervisor: Ivan Skorvánek
Second Supervisor: Bart van der Sloot

‘’The government is doomed to lose the fight, but nevertheless the fight goes on’’[1]

[1] Jay Stanley, ‘’Caspar Bowden Political Panel, Encryption of Communications and E-evidence’’ (Computers, Privacy and Data Protection Conference, Brussels, 26 January 2018).

Table of contents

CHAPTER 1
INTRODUCTION

1.1 Background

Communication through electronics are playing a crucial part in our lives and in society nowadays. Given that we increasingly communicate with each other electronically and that it contains vast amounts of information, it was foreseeable that interception of these communications would become a key focus in covert surveillance.[2] Covert surveillance on electronic communication started around 1950s with the classic interception of telephones, and since the 1990s it also includes the interception of online communications. This was due to the diversification of communications: not only telephone calls were made to communicate, but also email, instant messaging, etc. It was also due to the privatisation of the state operated telecommunication sectors which resulted in less cooperation with the police.[3] The privatisation started in the US, but many countries followed. However, electronic communications in this increasingly digital world is not always easy to intercept for law enforcement. This is mainly due to the increase of encryption of communication data. Different kinds of encryptions come with different kinds of problems. Regarding interception of electronic communications, one could think of end-to-end encryption and link encryption. With end-to-end encryption, the data is encrypted from one end device to the other end device without being decrypted at intermediate points. With link encryption, the data is encrypted as well but is decrypted and encrypted again at every intermediate point, often by routers when one is browsing on the internet. What is left for law enforcement to intercept are often the metadata, e.g. time, and location, but also the DNS queries which shows the domain names of websites visited.[4]

Apple was the first big company that started using end-to-end encryption in its iMessage app in 2011. [5] However, only after Edward Snowden's revelations in 2013 there was a huge increase of the use of encryption. For example, Yahoo immediately increased its encryption to keep the data away from the surveillance of law enforcement and secret services.[6] It wanted to encrypt all data which were flown to and from Yahoo. In 2016, WhatsApp announced that it was also going to use end-to-end encryption for all its data, which makes it impossible for the government to intercept these types of communications. [7] Moreover, popular VoIP's such as FaceTime and WhatsApp Voice Calls are also encrypted nowadays which makes the classic government wiretap more and more useless.[8] Furthermore, according to Mozilla, more than half the volume of the internet traffic in 2017 is encrypted.[9] So, when someone is visiting a website, it is more likely than not that it is visiting a HTTPS link encrypted website. This is just a small selection of measures that companies are taking to increase their encryption, but one can argue that we are slowly entering a new era of encryption by default, where ''encryption

---

[2] Gerald Chan. "Life after Vu: Manner of Computer Searches and Search Protocols. *"The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference* 67. (2014).
[3] Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 Mich. Telecomm. & Tech. L. Rev. 115 (2005).
[4] S. Bortzmeyer, *DNS Privacy Considerations*, Internet Engineering Task Force, August 2015, page 3.
[5] Apple, *''New Version of iOS Includes Notification Center, iMessage, Newsstand, Twitter Integration Among 200 New Features''* (6 June 2011) Press Release.
[6] Yahoo, *''Our Commitment to Protecting Your Information''* (18 November 2013) Press Release.
[7] WhatsApp, ''End-to-end encryption'' <https://faq.whatsapp.com/en/general/28030015> accessed 16 April 2018.
[8] For example, see Apple, ''This is how we protect your privacy'' <https://www.apple.com/privacy/approach-to-privacy/> accessed 21 April 2018.
[9] Let's Encrypt, ''Let's Encrypt Stats'' <https://letsencrypt.org/stats/> accessed 16 April 2018.

first'' is becoming the new norm for companies when dealing with technology.[10] But as said, when the encryption is done well enough one can basically not decrypt it. For example, in the Netherlands the new controversial Act on the Intelligence and Security Services 2017 extends the powers of Dutch intelligence services to intercept electronic communication data en masse, not only the suspect.[11] It permits the Dutch intelligence service to use techniques such as "investigation-mandated interception" of data. Law enforcement and intelligence services used to go to a service provider and ordered them to give them all the data of a suspect. Within the power of the investigation-mandated interception of data, they can demand the service providers to transfer a big amount of their customers' data to them at once. However, these ISP's are not able to decrypt the communication either and can merely hand over the metadata. The government may have a wide range of possibilities to intercept electronic communication data, but only up to a point where there is no encryption. There are rumours going on that in the future quantum computers will be able to crack the encryption, but at the same time there are already people working on quantum-safe cryptographies. So, decryption is basically impossible. Therefore, the question remains how law enforcement should adapt to this when they want to intercept electronic communication data.[12] What can they do? You do not want to ask the suspect directly for the communication data either, because then they know their data is being intercepted and it will set aside the whole purpose of covert surveillance. One frequently mentioned workaround would be the use of backdoors in these encrypted electronic communications. This would be a secret key that companies of electronic communications create for law enforcement, so they can decrypt it.

1.2 Problem statement

Encryption often leads to much frustration among governments around the world and has become a legal issue in recent years. However, most of the existing academic literature overlooks this problem entirely and merely focusses on overt surveillance and problems that may arise when law enforcement encounters an encrypted device. This merely covers the physical problems governments are experiencing when trying to get access to a device in the context of search and seizure. One could think of a missing pin code, password or fingerprint. However, device encryption is something different then end-to-end encryption and link encryption that secures communications in transit, rather than stored data on hardware.

Koops already discussed the possible methods of bypassing encrypting in 1999.[13] Although his PhD thesis is mainly about device encryption, he also discusses data interception such as wiretapping and interception of SMS texts. However, he does not mention encryption as a technical problem: ''not many cases are known of criminal

[10] Serdar Yegulalp, ''Welcome to the era of encryption by default'' (*InfoWorld*, 21 November 2013) <https://www.infoworld.com/article/2609941/encryption/welcome-to-the-era-of-encryption-by-default.html> accessed 16 April 2018.
[11] Explanatory Notes to the Act on the Intelligence and Security Services 2017, para 3.3.4.4.7.4.
[12] Kevin Bankston, ''Ending the Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors'' (*Lawfare* 14 June 2017) < https://www.lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors> accessed 16 April 2018.
[13] Bert-Jaap Koops, ''The Crypto Controversy: A Key Conflict in the Information Society'' (Kluwer Law International 1999).

organizations using encrypted communications.''[14] However, he does a prediction that in the future this might change: ''As far as transport is concerned, financial transactions, teleworking, video conferencing, and other types of communications will increasingly be encrypted for confidentiality. Supposing that mobile phones and data communications can in the future regularly be tapped, criminal organizations and computer criminals, with their knowledge of computer technologies, are likely to shift to encryption in order to remain outside the reach of wiretaps. Then, encryption for escaping law enforcement will be used on a larger - or even large - scale.''[15] This could be due that this research was done in 1999 and much of the communications were not encrypted yet. In 2012, he researched the same topic again, but focussed entirely on decryption methods in the case a device is encrypted.[16] Other authors did the same. One could think of the huge debates that arose after prominent cases such as the famous Apple vs. FBI case, or the Riley v. California case in which the court stated that warrantless seizure and search on a smartphone violates the suspects privacy.[17] Authors jumped on these cases. For example, Dan Froomkin and Jenna Mclaughlin argued that the FBI vs. Apple case established a new phase of crypto wars.[18] Gregory Coutros started to do research on the implications of creating backdoors in iPhones.[19] But as said before, most of the authors ignored the other side of investigation powers. End-to-end encryption and link encryption are hindering surveillance of electronic communications more and more. Even companies of online messaging apps using end-to-end encryption cannot see the message or has any way of decrypting it. There is no readable version available. If law enforcement demands access, there is simply nothing for the company to hand over.

The few authors that are discussing ways to bypass encrypted communications and in particular backdoors, do not thoroughly consider the risks or do not come up with a solution. Christopher Soghoian focused on the use of backdoors in encrypted communications in the US and argued that there are several laws and cases in the US which can be used to justify the insertion of backdoors in products. According to him, any firm can be compelled to insert a backdoor into its own product, no matter how committed it is to protect the privacy of its customers. [20] He continued with providing non-legal solutions for companies to avoid compelled backdoors. However, he only assumed that the US government can force companies to use backdoors to intercept data. Most countries cannot force companies to do the same. What if China approves backdoors and Germany does not, while their inhabitants both use the same application to communicate? Moreover, he does not consider the actual risks of backdoors in encrypted communications, let alone the alternatives of backdoors in encrypted

[14] Ibid 64.
[15] Ibid 89.
[16] Bert-Jaap Koops, ''The Decryption Order and the Privilege Against Self-Incrimination. Do developments since 2000 suggest a need to force suspects to decrypt?'' (Boom Lemma 2012).
[17] Supreme Court of the United States, Riley v. California, United States Reports 573 (2014).
[18] Dan Froomkin & Jenna McLaughlin, ''FBI VS. Apple establishes a new phase of the Crypto Wars'' (*The Intercept* 26 February 2016) < https://theintercept.com/2016/02/26/fbi-vs-apple-post-crypto-wars/> accessed16 April 2018.
[19] Gregory Coutros, 'The Implications of Creating an iPhone Backdoor.' (2016) 6(2) Nat'l Sec L Brief 81, p. 81-84.
[20] Christopher Soghoian, Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era (August 17, 2009). 8 J. on Telecomm. and High Tech. L. 359; Berkman Center Research Publication No. 2009-07, p. 411.

communications. Peter Swire and Kenesa Ahmad do partly discuss the major technical and legal risks associated with backdoors in encrypted communications, in particular the jurisdiction problem. [21] Consequently, they reject the idea of a backdoor and instead of coming up with a solution, they conclude that there is no ‘’going dark’’ problem since there is a lot of new information available that can replace the content of communications. However, the jurisdiction problem could be seen as merely an obstacle that one can overcome when evaluating if backdoors are a proportionate solution. Moreover, they do not take into consideration that the collection of these metadata can constitute a serious privacy violation, even more then if backdoors were implemented. Furthermore, their research is done in 2012 and did not consider the increasing use of encryption and the law enforcement protests afterwards which occurred because of Edward Snowden’s revelations. Nevertheless, the jurisdiction problem and the mapping of metadata will be critically discussed in Chapters 3 and 4. The Law Library of Congress came up with a comparative report on government access to encrypted communications in different countries.[22] However, despite its title this research again mainly focused on warrants to search encrypted devices and decryption orders, while only citing some institutions and persons who are also against backdoors in communication data. Orin S. Kerr & Bruce Schneier specifically researched and categorised the workarounds of encryption and came up with backdoors as one of the alternatives.[23] However, their workarounds are again mainly focussed on device encryption and their description of ‘’deliberately inserted flaws’’ is kept short. Nevertheless, their analysis of workarounds is also useful to look at when looking for ways to bypass encrypted electronic communications. This will be done in Chapter 4. The EDRi came with a response on Kerr’s and Schneier’s paper. In its response, it assessed the workarounds in a digital rights perspective, to emphasize the importance of putting in place strong and specific safeguards regarding every encryption workaround. However, in its paragraph about flaws as a workaround it focused on hacking instead, while completely disregarding the use of backdoors.[24] Finally, a group of pre-eminent computer scientists and cryptographers came up with a report in 2015 which was focussed on backdoors in encryption, and half of their research was in the context of backdoors in encrypted communications.[25] They came up with a profound analysis of the risks of backdoors in these communications, and concluded that at present time, backdoors should not be considered due to these inherent risks. Furthermore, they came up with several procedural and administrative questions on specifications of the system in the case the demand for exceptional access is to be taken seriously.[26] However, their report is primarily focused on the argument that exceptional access is a bad idea from a

[21] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157.
[22] The Law Library of Congress, ‘’Government Access to Encrypted Communications’’ (*Global Legal Research Center* May 2016) <https://www.loc.gov/law/help/encrypted-communications/index.php> accessed 16 April 2018.
[23] Orin S. Kerr and Bruce Schneier, Encryption Workarounds (March 20, 2017). Georgetown Law Journal, Forthcoming; GWU Law School Public Law Research Paper No. 2017-22; GWU Legal Studies Research Paper No. 2017-22, p. 22-23.
[24] EDRi, *’’Encryption Workarounds. A digital rights perspective’’* (12 September 2017) p. 8-9.
[25] Abelson et al., 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026.
[26] Ibid 20-24.

technical perspective. The risks they come up with can be mitigated, which allows for a more balanced approach on this topic. They did not consider any alternative as well.

Even though the actual proportionality of backdoors in encrypted electronic communications is still more or less uncovered in academic literature, governments continue to struggle with their incapability to keep track of what people are communicating when intercepting electronic communications. For example, in 2016 the EU Member States indicated that in about 75% of the cybercrime investigations there was some form of encryption in communication involved, which hindered the government for gaining evidence.[27] In January 2015, UK Prime Minister David Cameron stated that he wants to introduce a ''comprehensive piece of legislation'' that makes sure we do not allow terrorists ''safe spaces'' to communicate with each other.[28] His successor Theresa May is stating the same.[29] In 2017, the Home Secretary of the UK Amber Rudd announced that it wanted to have access to all secure communications like WhatsApp and Snapchat.[30] She stated that it was "completely unacceptable" that the law enforcement and intelligence services are not able to read messages protected by end-to-end encryption. Australia also states that safe backdoors are feasible.[31] In 2016, The German intelligence services even announced that it wants to spend €150 million to modernize its capabilities to crack the encryption of messaging services like WhatsApp to make interception of electronic communications easier.[32] Moreover, the Trump administration stated in January 2017 that it wanted to force tech companies to create backdoors in their encryption.[33] They stated that ''It is also critical, however, that national security and criminal investigators can overcome encryption, under lawful authority, when necessary to the furtherance of national-security and criminal investigations.'' As far as tech companies such as Google and Yahoo are concerned about these statements, there is no guarantee for how long they would deny the backdoor demands from governments. However, in 2016 the Dutch government stated that it does not want to limit the ongoing encryption of data for now, e.g. by forcing companies to create backdoors in their technology.[34] They said that backdoors in these systems would make these systems vulnerable for terrorists, foreign intelligence

[27] Europol ''*Director's speech at the Conference: privacy in the digital age of encryption and anonymity online''* (19 May 2016) Press Release.
[28] BBC News, ''David Cameron says new online data laws needed'' *BBC News* (London, 12 January 2015) <http://www.bbc.com/news/uk-politics-30778424> accessed 16 April 2018.
[29] Alex Hern, ''May calls again for tech firms to act on encrypted messaging'' *The Guardian* (London, 25 January 2018) <https://www.theguardian.com/technology/2018/jan/25/theresa-may-calls-tech-firms-act-encrypted-messaging> accessed 16 April 2018.
[30] Andrew Sparrow, ''WhatsApp must be accessible to authorities, says Amber Rudd'' *The Guardian* (London, 26 March 2017) <https://www.theguardian.com/technology/2017/mar/26/intelligence-services-access-whatsapp-amber-rudd-westminster-attack-encrypted-messaging> accessed 16 April 2018.
[31]Nick Evershed, ''Australia's plan to force tech giants to give up encrypted messages may not add *up'' The Guardian* (London, 14 July 2017) <https://www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up> accessed 16 April 2018.
[32] Andre Meister, ''Projekt „ANISKI": Wie der BND mit 150 Millionen Euro Messenger wie WhatsApp entschlüsseln wil'' (*Netzpolitik*, 29 November 2016) < https://netzpolitik.org/2016/projekt-aniski-wie-der-bnd-mit-150-millionen-euro-messenger-wie-whatsapp-entschluesseln-will/> accessed 16 April 2018.
[33] Chris Kanaracus & Steve Wilson, ''Expect renewed push for encryption backdoors from Trump administration'' (*ZDNet*, 26 January 2017) < https://www.zdnet.com/article/expect-renewed-push-for-encryption-backdoors-from-trump-administration/> accessed 16 April 2018.
[34] Letter from the Ministry of Security and Justice to the President of the House of Representatives of the State's General. Cabinet's view on encryption (01-2016) 26643-383.

services and criminals. It would weaken the overall security of technology. This opinion is clearly swimming against the political mainstream. As of October 2017, it seems like their opinion did not change, since they did not mention the weakening of encryption in their coalition agreement.[35] However, it might be that they left this out on purpose, since these agreements usually do not go into such detail.

In June 2017, the European Commission also mentioned in its Eighth Progress Report for the first time the increasing challenges intelligence services and law enforcement encounter when dealing with encryption in investigations. [36] In its Eleventh Progress Report, it continues by stating that the use of encryption is expected to grow further in the coming years.[37] Therefore, in this Progress Report the Commission came up with an anti-terrorism package for law enforcement, which includes technical and legal measures to support law enforcement in criminal investigations. It will apply to both encrypted devices and encrypted electronic communications. It wants to do this without ''prohibiting, limiting or weakening encryption.'' However, it is unclear what the Commission means when it stated that it was not proposing measures that could ''limit or weaken encryption", since this usually is the case when law enforcement is trying to bypass encryption. Chapter 4 will critically reflect on the Commission's anti-terrorism package, but it seems like it is struggling to find a position on encryption. [38]

[35] People's Party for Freedom and Democracy (VVD), Christian Democratic Alliance (CDA), Democrats '66 (D66) and Christian Union (CU), ''Confidence in the Future: 2017-2021 Coalition Agreement'' (10 October 2017).
[36] Commission, ''Communication from the Commission to the European Parliament, the European Council and the Council, Eighth progress report towards an effective and genuine Security Union'' COM (2017) 354 final,
p. 6.
[37] Commission, ''Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union'' COM (2017) 608 final, p. 8
[38] Joe McNamee, ''The European Commission struggles to find a position on encryption'' (*EDRi* 31 October 2017) < https://edri.org/european-commission-struggles-find-position-encryption/> accessed 16 April 2018.

1.3 Research question

To what extent are backdoors in encrypted electronic communications such as HTTPS and WhatsApp a proportional solution to the problem that the use of encryption by criminals poses to law enforcement, particularly as it relates to covert surveillance?

1.3.1 Sub-questions

1) How to define what is proportional? Creating a legal framework.
    a. Necessary in a democratic society
    b. The proportionality principle
    c. Conclusion
2) What are backdoors? An analysis of backdoors in encrypted electronic communications.
    a. Function of backdoors
        i. Definition
    b. The risks associated with backdoors
        i. Exploitation by malicious parties
        ii. Complexities
        iii. Costs
        iv. Extraterritorial application
        v. Avoidance

    Conclusion
3) What are the alternatives to bypass encrypted electronic communications? An overview of alternatives.
    a. Purpose
    b. A taxonomy of encryption workarounds
        i. Hacking
        ii. Seizure of backups in the cloud
    c. Mapping of metadata
    d. Other possible alternatives
    e. The European Commission's anti-terrorism package
    f. Conclusion
4) To what extent are backdoors a proportional solution? The evaluation of backdoors in encrypted electronic communications.
    a. The proportionality principle
    b. Mitigation of the risks
    c. A different approach

1.4 Significance

There is clearly a gap in the literature regarding the proportionality of backdoors in encrypted electronic communications. Most of the literature regarding this topic is focused on the other side of surveillance, namely backdoors in encrypted devices in the context of search and seizure. The literature that do focus on backdoors in encrypted electronic communications often comes up with resolvable risks or immediately rejects the use of backdoors without assessing the proportionality by coming up with other alternatives that could solve the encryption problem. However, governments still vehemently complain and protest about encryption in these communications and the European Union also realizes something needs to happen but it does not know exactly how it should tackle this problem. Regular criminal investigations are not being pursued, because the evidence can't be encrypted by law enforcement. To be clear, it covers a variety of crimes, not necessarily cybercrimes. Therefore, law enforcement wants measures to bypass encrypted electronic communications, but this entails strong opposition from companies, civil liberty campaigners and digitally minded countries like the Netherlands. In any case, it is inevitable that the law must come up with a solution because even more communications will be encrypted in the future. A more balanced approach is needed. This approach would help law enforcement to intercept communications and protect society from terrorists and criminals, but at the same time respect people's privacy which also entails protection of communications. Therefore, this research wants to critically evaluate to what extent the use of backdoors as one of the workarounds for encrypted communications is a proportional solution to the problem that the use of encryption by criminals poses to law enforcement. The framework of proportionality of art. 8 ECHR will be used, since we must realize that it is not just encryption as a technology that is preventing access to data, but also the law. It will examine interception by law enforcement and does not include intelligence services although they both face the same problems regarding encryption in electronic communication data. However, they both use a different framework for privacy infringements. Law enforcement is supervised by legal authorities according to legal procedures, intelligence services are supervised trough political procedures and fall outside the scope of EU treaties. This means that law enforcement actions could be tested at a court, which entails more public data to be available regarding criminal investigations. On the other hand, intelligence services' investigations are unclear and not publicly available. For example, NSA's secret interception and decryption methods such as PRISM, FAIRVIEW and BULLRUN are only known due to whistle-blowers. These methods will not be discussed. Koops confirms this when it stated that until the mid-1990s the encryption debate was centralized for a large part around intelligence services, but that it has gradually shifted towards law enforcement interests.[39]

1.5 Methodology

This research will focus on the analysis and evaluation of backdoors in encrypted electronic communications when governments are unable to intercept these communications. This section describes step-by-step how the evaluation of backdoors in encrypted electronic communications as a proportional solution is going to be conducted. Throughout this research a doctrinal legal method is used to get a full

[39] Bert-Jaap Koops, *''The Crypto Controversy: A Key Conflict in the Information Society''* (Kluwer Law International 1999), p. 3.

understanding of the rationale and risks of backdoors that are described in academic literature, as well as the alternatives that could fulfil the same purpose as backdoors.

In Chapter 2, a framework is created of what constitutes the proportionality principle which is part of the ‘’necessary in a democratic society’’ requirement of art. 8 ECHR. How is this principle defined by the ECtHR and does academic literature have different opinions on this principle? Accordingly, a critical evaluation can be performed regarding the use of backdoors.

In Chapter 3, a profound analysis of the whole concept of backdoor is conducted. What is its function, and what are the advantages and risks of the use of backdoors? This analysis might also reveal the problems that may arise if countries have different approaches regarding backdoors. What if e.g. the US is forcing companies to use backdoors in their encryption, while in Europe the ePrivacy Regulation might get ratified with a provision stating that all backdoors are prohibited? This will clearly entail a clash between countries, since the same electronic communication might be used in different countries. Moreover, are backdoors needed to keep track of electronic communications and to correspond to the governments complaints, or is it just a new method to ease surveillance that complements the other powers at the expense of the security and protection of communication? This Chapter will specifically look the insights of Peter Swire and Kenesa Ahmad as laid down in their paper, which in particular examined the clash of jurisdictions and the lack of trust in other countries thereof.[40]

After the analysis of the use of backdoors by law enforcement, Chapter 4 will consider the alternatives that serve the same purpose as backdoors. Are there other alternatives that can bypass encrypted electronic communications and which are less intrusive? This will mainly be done by looking at the taxonomy of workarounds as laid down by Orin S. Kerr & Bruce Schneier. [41] They came up with six different workarounds, however only the last two workarounds are especially relevant for bypassing encrypted communications. These consist of getting access to plaintext when the device is in use and locating a plaintext copy of the sought-after data. Nonetheless, their taxonomy is still useful to get inspiration and gain insight in the different possibilities of conducting communication surveillance when encryption is involved. For example, The Netherlands has started significant reforms to adapt to the technological developments, such as art. 126nba in the proposed Computer Crime III Bill to hack into computers of suspects.[42] Their taxonomy will make it clearer to understand if there are better solutions available rather than forcing companies to introduce backdoors in their encryption. Besides the workarounds as laid down by Orin S. Kerr & Bruce Schneier, other alternatives that Orin S. Kerr & Bruce Schneier did not assess will also be discussed. Finally, a critical analysis of the Commission’s proposed anti-terrorism package for law enforcement will also be conducted.

[40] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157.
[41] Orin S. Kerr and Bruce Schneier, Encryption Workarounds (March 20, 2017). Georgetown Law Journal, Forthcoming; GWU Law School Public Law Research Paper No. 2017-22; GWU Legal Studies Research Paper No. 2017-22.
[42] Explanatory Notes to the proposed Computer Crime III Bill, p. 98.

In Chapter 5, the framework that is discussed in Chapter 2 will be applied to evaluate backdoors and the alternatives that are discussed in Chapters 3 and 4. Moreover, it will come up with a plausible solution to the problem if backdoors fail to meet to the proportionality requirement of art. 8 ECHR, or if this is necessary in any other way. Chapter 6 will be devoted for the conclusion.

CHAPTER 2 LEGAL FRAMEWORK

2.1 Creating a framework

The use of covert surveillance such as intercepting communication constitutes an interference with art 8 ECHR.[43] This way, a backdoor primarily acts as a supporting power to collect data which would end up in the hands of law enforcement anyway through interception. This is similar to a decryption order in the case a device is encrypted.[44] This research already assumes that there is a justified interference with art. 8 ECHR when communications are intercepted. Therefore, the implementation of a mandatory backdoor does not or only scarcely intrude on art. 8 ECHR, since the permission to intercept already implies that the corresponding adequate and sufficient safeguards are met and that data can be lawfully collected.[45] Consequently, this research will not e.g. discuss the scope, duration and supervision of interception or remedies against it. However, in the case communications are encrypted, law enforcement must find a way to bypass these encrypted data. There are several ways to achieve this, but these workarounds should also be justified. Therefore, using backdoors to bypass this barrier which facilitates interception still violates art. 8 ECHR if the use of backdoors is not justified.[46] Thus, we need to create a framework to evaluate this. The issue of encrypted electronic communications is a problem of balancing. On the one side, there are the legitimate interests of law enforcement, and on the other side there are legitimate interests of people to have their privacy and communications respected. The ECtHR uses the older term "correspondence" for this in art. 8 ECHR, but this term is interpreted broadly to include newer forms of communication as well, such as instant messaging and email.[47] Art. 7 EU Charter does have the term ''communications'' laid down. However, the ECtHR can reasonably be considered as the most important human rights court in Europe, since it sets the minimum standards for human rights in the European Union, and case law from the ECtHR has also significance for the European Court of Justice who must interpret the EU Charter.[48] Therefore, this research will use the doctrine of art. 8 ECHR and the Courts interpretation thereof.

2.2 Necessary in a democratic society

Both interests clearly clash, and to evaluate whether backdoors are a solution we need to create a framework first. As a basis for the framework, the doctrine considered by the ECtHR is used as the Court considered this issue in depth. The fundamental right to the respect for private life provided for in art. 8 ECHR is not absolute, and might be limited if the requirements in art. 8 par. 2 ECHR are met. Therefore, a backdoor must be in accordance with a law, is in pursuit of the legitimate interests listed in art. 8 par. 2

---

[43] Klass and Others v Germany App no 5029/71 (ECtHR, 6 September 1978), par. 41. See also Malone v the United Kingdom App no 8691/79 (ECtHR, 2 August 1994), par. 64 and Kruslin v France App no 11801/85 (ECtHR 24 April 1990), par. 26.

[44] In The Netherlands this debate resulted in a proposal to implement a data decryption obligation for suspects in the new Computer Crime Act III, but the Council of State rejected this idea because it was in contrary to the principle of nemo tenetur. See *Kamerstukken II* 2015/2016, 34 372, nr. 4.

[45] Bert-Jaap Koops, ''The Decryption Order and the Privilege Against Self-Incrimination. Do developments since 2000 suggest a need to force suspects to decrypt?'' (Boom Lemma 2012), p. 24.

[46] OHCHR, ''Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye'', 22 May 2015, UN. Doc. A/HRC/29/32, p. 11.

[47] Bert-Jaap Koops et al., A Typology of Privacy (March 24, 2016). University of Pennsylvania Journal of International Law 38(2): 483-575 (2017); Tilburg Law School Research Paper No. 09/2016.

[48] Michael Friedewald et al., *''Surveillance, Privacy and Security: Citizens' Perspectives''* (Routledge 2017), p. 159-160.

ECHR, and the measure must be necessary in a democratic society.[49] However, this framework will specifically focus on one of the requirements, namely the necessary in a democratic society, since the first two requirements are usually not disputable. The necessity test has been the only test for a long time and is also laid down in the Convention.[50] However, nowadays the Court also uses different tests to deals with the third requirement of art. 8 par 2. ECHR. The most common tests are the original necessity test, but also the balancing test, the Pareto efficiency and the in abstracto approach.[51] Nowadays, the balancing test is the most dominant framework under the ECHR and ECtHR.[52] However, regarding national security and prevention of crime cases, the necessity test is often still used.[53] In these cases, the Court usually does not so much weigh the private interests of the individuals involved, but focuses primarily on the factual necessity of the infringement. That the Court is willing to let the individual interests override is understandable, because security is the basis of society and it is in everyone's interest to have a secure environment, even though there is an interference. In other words, there is no conflict between the interests. Therefore, in such cases, the Court merely asks the question whether the infringement is necessary in a democratic society. Subsequently, this research will use the same necessity test, since backdoors in encrypted electronic communications are measures to ensure national security and prevent crime.

In the Handyside v. the United Kingdom case, the ECtHR clarified that the term "necessary" is not synonymous with ''indispensable'', ''absolutely necessary'' or ''strictly necessary'', but that there should be a ''pressing social need''.[54] It explained necessity in this context of art. 10 ECHR, but it is also useful for other articles. However, in Klass and others v. Germany the ECtHR later explicitly states that in the context of covert surveillance, interferences of art. 8 ECHR are only allowed if they are ''strictly necessary''. [55] This is due that covert surveillance could easily be abused and undermine or even destroy democracy. [56] Moreover, in Szabó and Vissy v Hungary case, the Court specifically states with regards to covert surveillance that the measure should not only be strictly necessary, but must be only allowed to ''obtain essential intelligence in an individual operation''.[57] Thus, the pressing social need requirement is not used here, but the strictly necessity requirement and merely individual operations instead. In line with this, the court stated that there must be adequate and effective

[49] A.J. Nieuwenhuis et al*., ''Hoofdstukken Grondenrechten''* (3th edition, Ars Aequi Libri 2014), p. 96.
[50] Bart van der Sloot, ''The Practical and Theoretical Problems with 'balancing': Delfi, Coty and the Redundancy of the Human Rights Framework'' (2016) 23 (3) Maastricht Journal of European and Comparative Law, p. 440.
[51] Ibid. See also Steven Greer, '*'The exceptions to Articles 8 to 11 of the European Convention on Human Rights''* (Council of Europe Publishing 1997), p. 15 and 23.
[52] Bart van der Sloot, ''Ten Questions about Balancing'' (2017) 3 (2) EDPL, p. 190, and Bart van der Sloot, ''The Practical and Theoretical Problems with 'balancing': Delfi, Coty and the Redundancy of the Human Rights Framework'' (2016) 23 (3) Maastricht Journal of European and Comparative Law, p. 441.
[53] For example, Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016), par. 54 and Kennedy v the United Kingdom App no 26839/05 (ECtHR, 18 August 2010), par. 130.
[54] Handyside v the United Kingdom App no 5493/72 (ECtHR, 7 December 1976), par. 48.
[55] Klass and Others v Germany App no 5029/71 (ECtHR, 6 September 1978), par. 42, 48 and 56. See also Weber and Saravia v Germany App no 54934/00 (ECtHR, 29 June 2006), par. 42 and Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000), par. 47.
[56] Klass and Others v Germany App no 5029/71 (ECtHR, 6 September 1978), par. 49
[57] Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016), par 72-73.

guarantees against abuse in the case of covert surveillance.[58] However, in more recent jurisprudence the court explicitly states that the examination of adequate and effective safeguards belongs to the in accordance with the law requirement.[59] In the Roman Zakharov v. Russia case the Court nicely summarises the requirements needed for safeguarding against abuse.[60] However, as this case belongs at the law requirement now, this thesis will not discuss it further. In the Handyside case, the Court further gives a second requirement of the notion of necessity. The reasons given by law enforcement to justify the interference must not only be strictly necessary, but also ''relevant and sufficient''.[61] Moreover, it also gives a third requirement which entails that the interference must be proportionate to the legitimate aim pursued.[62]

Therefore, the Council of Europe's Recommendation on Internet Freedom stated that ''interference with anonymity and confidentiality of communications is subject to the requirements of legality, legitimacy and proportionality of Article 8 ECHR.''[63] In Segerstedt-Wiberg and Others v. Sweden the court explicitly states that these three requirements are even more important in the context of covert surveillance.[64]

2.3 The principle of proportionality

This framework will focus on the principle of proportionality, since this is the most prominent principle out of the three Handyside-standards.[65] This prominence can also be derived from case law.[66] Summarized, the use of backdoors must be proportionate to the legitimate aim of fighting crime.[67] This will vary from case to case, the different circumstances considered, the fundamental right in question and the type of interference. As we are not using the balancing test, the proportionality principle does not imply a balancing exercise as such.[68] In these cases, the Court increasingly uses the

[58] Klass and Others v Germany App no 5029/71 (ECtHR, 6 September 1978), par. 50 and 55. See also Kennedy v the United Kingdom App no 26839/05 (ECtHR, 18 August 2010), par. 153 and Roman Zakharov v Russia App no
47143/06 (ECtHR, 4 December 2015), par. 232
[59] Malone v the United Kingdom App no 8691/79 (ECtHR, 2 August 1994), par. 67.
[60]Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), par. 227-303.
[61] Handyside v the United Kingdom App no 5493/72 (ECtHR, 7 December 1976), par. 50.
[62] Ibid par. 49. For more recent examples regarding art. 8 ECHR see Üner v The Netherlands App no 46410/99 (ECtHR, 16 October 2006), Slivenko v Latvia App no 48321/99 (ECtHR, 9 October 2003), par. 91, Lee v the United Kingdom App no 25289/94 (ECtHR, 18 January 2001) and Z v Finland App no 22009/93 (ECtHR, 25 February 1997), par. 94.
[63] Recommendation CM/Rec(2016)5 of the Committee of Ministers of the Council of Europe to member States on Internet Freedom, 13 April 2016, par. 4.1.7.
[64] Segerstedt-Wiberg and Others v Sweden App no 62332/00 (ECtHR, 6 June 2006), par. 88.
[65] F.M.C. Vlemminx, *''Het moderne EVRM''* (Boom Juridsche Uitgevers 2013), p. 221. See also David Harris et al., *''Law of the European Convention on Human Rights''* (3rd edition, Oxford University Press 2014), p. 349.
[66] For example, Uzun v Germany App no 35623/05 (ECtHR 2 October 2010), par. 78: "In determining whether the applicant's surveillance via GPS as carried out in the present case was 'necessary in a democratic society', the Court reiterates that the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued."
[67] FRA, *''Fundamental Rights Report 2017''* (May 2017) p. 166.
[68] Bart van der Sloot, ''Ten Questions about Balancing'' (2017) 3 (2) EDPL, p. 189.

‘’less restrictive means’’ reasoning. [69] In other words, the proportionality principle should examine whether a backdoor in encrypted communications is ‘’the least intrusive instrument amongst those which might achieve the desired result’’.[70] Are there other laws or policies thinkable, that are equally effective, but less infringing?[71] The measure must also target a specific objective and not unduly infringe other fundamental rights of the targeted persons.[72] Regarding backdoors in encryption, one could think of freedom of expression. Moreover, the proportionality principle must examine the high risk that vulnerabilities in the security of encryption can be exploited by criminals and terrorists, notably the same as the measure is focussing on.[73] Further implications of the principle of proportionality used by the ECtHR remain obscure and, with some notable exceptions, the Court has been hesitant to provide further clarification.[74] This is also the case with the other parts of the necessity test.[75] However, a certain amount of uncertainty is inherent to the use of open norms. How this open norm of proportionality is filled in, depends on the societal developments at a certain time. This has the advantage that open norms can follow these societal developments in a fast pace. Nevertheless, to critically evaluate the use of backdoors by using the proportionality framework, law enforcement must have sufficient information on this measure, as well as other possibilities which serve the same purpose. This is also the conclusion of Jonida Milaj in her article on surveillance and proportionality.[76]Therefore, the next Chapters will analyse the use of backdoors, as well as examine other alternatives.

2.4 Conclusion

For the framework to evaluate to what extent backdoors are a proportionate solution, this research is using the doctrine as laid down by the ECtHR and academic literature. In this regard, we should evaluate whether the use of backdoors is the least intrusive solution to the problem that the use of encryption by criminals poses to law enforcement. Furthermore, backdoors should not unduly infringe other fundamental rights. Finally, this research will examine the high risk that breaches in the security of encryption might be exploited by criminals and terrorists as well.

---

[69] Brems, Eva and Lavrysen, Laurens, ‘Don't Use a Sledgehammer to Crack a Nut’: Less Restrictive Means in the Case Law of the European Court of Human Rights (January 2015). Human Rights Law Review 15 (1), 2015, 1-30.

[70] UN Human Rights Committee (HRC*), CCPR General Comment No. 27: Article 12 (Freedom of Movement*), 2 November 1999, CCPR/C/21/Rev.1/Add.9, par. 14

[71] De Hert, P. 2005. “Balancing Security and Liberty within the European Human Rights Framework. A Critical Reading of the Court’s Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies After 9/11.” Utrecht Law Review 1 (1): 68 –96.

[72] OHCHR, ‘’Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye’’, 22 May 2015, UN. Doc. A/HRC/29/32, p. 12.

[73] Ibid.

[74] Steven Greer, *‘’The exceptions to Articles 8 to 11 of the European Convention on Human Rights’’* (Council of Europe 1997), p. 14.

[75] ibid

[76] Milaj, Jonida, *Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance*. In: International Review of Law, Computers & Technology. 2016; Vol. 30, No. 6. pp. 115-130.

CHAPTER 3
ANALYSIS OF BACKDOORS

3.1 Rationale

Encryption as a mathematical function constitutes of two different models. For symmetric encryption, a secret value - the key - is used to encode data so that only users with access to that key can decode the information''.[77] The same key is used to encrypt and decrypt data. However, end-to-end encryption is an asymmetric encryption. In this case, two different keys are used: one key is used to encrypt data and another key is used to decrypt data. Only the intended recipient can read the electronic communication using a unique key. In either way, if law enforcement is trying to intercept such communication in transit, they are simply not able to read the content of the communication without having the key. It makes the intercepted data useless; what they see is merely a random set of characters. Therefore, encryption safeguards our respect for private life and protects our communications against breaches of confidentiality, while also stimulating trust in digital infrastructures such as online banking, which is essential for innovation and economic growth.[78] The Art. 29 Working Party stated that strong and secure encryption is a security practice which ''aims to provide the confidentiality of communication channel between identified parties (human beings, devices, or pieces of software/hardware) to avoid eavesdropping or unintended disclosure''.[79] As already stated in Chapter 1, it became more difficult for law enforcement to technically intercept encrypted electronic communications. In 1997, James X. Dempsey already stated that there seems to be no way to limit the spread of virtually unbreakable encryption.[80] Therefore, it is argued by countries that companies should be obligated to implement backdoors into their encryption, to make it possible for law enforcement and intelligence services to continue with the interception of electronic communications. This way, terrorists and criminals cannot avoid detection and law enforcement will not miss out on evidence.[81] For this research, the definition of electronic communication is used as laid down in art. 2 ePrivacy Directive.[82]

3.1.1 Definition

When a programmer intentionally creates an undocumented portal into its encrypted system, this opening is called a ''backdoor''.[83] The metaphor is that the front door of a house is securely locked, but someone can enter through a backdoor that appears to be locked, but is easy to open. There are different stakes at risk. For example, a system administrator might want to retain access to all data and communications in a system to

[77] Information Commissioner's Office, ''Encryption'' (3 March 2016) p. 3.
[78] Maryant Fernández Pérez, ''EU's plans on encryption: What is needed?'' (*EDRi*, 16 October 2017) <https://edri.org/eus-plans-on-encryption-what-is-needed/> accessed 20 April 2018.
[79] Art. 29 Working Party (2014), Opinion 05/2014 on Anonymization Techniques, WP 216, Brussels, 10 April 2014, p. 29.
[80] James X. Dempsey, Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy, 8 Alb. L.J. Sci. & Tech. 65 (1997).
[81] FRA, *''Fundamental Rights Report 2017''* (May 2017) p. 158.
[82] Art. 2 (A): signals by wire, by radio, by optical or by other electromagnetic means. Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002) OJ *L201/37*.
[83] Kim Zetter, "Hacker Lexicon: What is a Backdoor" (*Wired*, 11 December 2014) <http://www.wired.com/2014/12/hacker-lexicon-backdoor/> accessed 20 April 2018.

ensure that organization policies are being followed.[84] This way, backdoors are used for maintenance or troubleshooting. Regarding interception of electronic communication by law enforcement, technology companies might be obligated by law to build backdoors into their systems to allow government access to the communication. For example, a messaging application that promotes encrypted communication might be obligated to have a technical vulnerability or security flaw built into its encryption algorithm that allows law enforcement to intercept these communications.

When intentionally creating vulnerabilities, the establishment of a "key escrow" regime is a well-known method. Regarding interception by law enforcement, the users of encryption would be obligated to store their keys at an escrow authority such as a governmental institution or independent third party, who hold copies of these encryption keys in trust. They must hand over the keys to law enforcement when certain legal conditions are fulfilled. [85] In other words, the keys would be held in "escrow''. For law enforcement, key escrow provides a way of allowing strong encryption for electronic communications while still having the power to intercept these communications. To prevent abuse, the government could for example establish two separate key escrow databanks, to be run by independent entities, each of which would hold one part of the key.[86] In case of a lawful court order for a suspect's communications, the two key escrow data banks must reveal their parts of the key to law enforcement which subsequently puts the two parts together to decrypt the communications. In this regime, communications of other people would remain encrypted and unavailable to law enforcement.[87] One of the first examples of a (hidden) backdoor with key escrow is the Clipper Chip proposed by Clinton in the 1993.[88] The Chip was promoted by the NSA as a hardware encryption device that would secure "voice and data messages'', however a decryption key was created and secretly held in escrow by the government which was then able to access telephone communications in the case lawful warrant was given. The government hoped that if enough people would voluntarily use this chip, the encryption problem would remain manageable. The police would simply notice when someone did not use such a Clipper, and this would be interesting information on its own. Ultimately the proposal became outdated as digital technology progressed. A more recent example can be found in Canada. Jordan Pearson and Justin Ling explained how the Canadian Police was able to intercept encrypted

[84] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 432.
[85] Privacy International, ARTICLE 19 and IHRC, ''*Securing Safe Spaces Online. Encryption, online anonymity, and human rights''* (17 June 2015).
[86] Statement by the Press Secretary, Office of the Press Secretary, The White House, ''The Clipper Chip Initiative'' (*EPIC*, 16 April 1993), <http://epic.org/crypto/clipper/white_house_statement_4_93.html> accessed 20 April 2018.
[87] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 435.
[88] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 434.

Blackberry messages between 2010 and 2012.[89] This was simply due that the government found the ‘’global encryption key’’ to decrypt all Blackberry messages.

However, a critical question should be asked in this regard. Do we have secure communications without backdoors 24 years later? Instant messaging apps like Signal, WhatsApp and iMessage are end-to-end encrypted, but if you make a phone call it is not end-to-end encrypted anymore. This is due that telephone systems are based on Signalling System No. 7, and SS7 is vulnerable for interception.[90] Moreover, many vendors advertise they use end-to-end encryption, but at the same time they keep a backup copy of one’s messages in the cloud, so one can load it into their device as a backup. As stated in Chapter 1, law enforcement is more concerned about stored data then communicated data. This could be derived from the tremendous focus on device encryption in academic literature. Stored data such as those backups in the cloud could be easily seized by law enforcement. An existing solution would be to turn of backups and trade convenience for security. This research will consider the seizure of cloud storage in Chapter 4.

3.2 Risks

The proportionality principle must also examine the risks that breaches in the security of encryption entail. As seen in Chapter 1, a prominent risk is that those breaches might be exploited by criminals and terrorists, which could notably be the same as the measure is initiated for. This is already the main argument opponents of backdoors use. However, there are more risks that can be associated with backdoors. First, this research will consider this most dominant risk, and after a profound analysis of this risk this research will consider the other risks, such as the complexity and the problem of jurisdiction. In either way, it must be mentioned that most critique on the use of backdoors are coming from computer scientists and cryptographers, rather than academic lawyers. According to these scientists, law enforcement access to encrypted data is technically impossible without undermining the security of our society. Other authors also discussed this issue. For example, the UN Special Rapporteur on the right to privacy stated that “the security risks introduced by deliberately weakened encryption are vastly disproportionate to the gains”. [91]

3.2.1 Exploitation by malicious parties

The main problem with backdoors is that from a technical point of view, encryption cannot be weakened ‘’just a little’’ without potentially introducing additional vulnerabilities.[92] When there is a vulnerability, anyone can take advantage of it, not just law enforcement. Sooner or later, a secret vulnerability will be exploited by a malicious user. This malicious user could as well be the same person whose communication is being intercepted for the sake of national security or prevention of crime. It is extremely

---

[89] Jordan Pearson & Justin Ling, ‘’Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages’’ (*Motherboard*, 14 April 2016) <https://motherboard.vice.com/en_us/article/mg77vv/rcmp-blackberry-project-clemenza-global-encryption-key-canada> accessed 20 April 2018.

[90] G. Lorenz, T. Moore, G. Manes, J. Hale and S. Shenoi, ‘’*Securing SS7 Telecommunications Networks’’* (January 2001), p. 273.

[91] OHCHR, ‘’Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci’’, 30 August 2016, UN. Doc. A/71/368, par. 32.

[92] Maryant Fernández Pérez, ‘’EU’s plans on encryption: What is needed?’’ (EDRi, 16 October 2017) <https://edri.org/eus-plans-on-encryption-what-is-needed/> accessed 20 April 2018.

difficult to install a backdoor that can be used by the good guys, such as authorized law enforcement, while keeping out the bad guys.[93] In the case of a key escrow regime, criminals or hackers can penetrate a key escrow databank and steal the master backdoor encryption key or collection of keys used for a certain communication. Consequently, they would be able to arbitrarily decrypt internet communications. Millions of governmental, corporate and personal secrets would suddenly become vulnerable to manipulation and theft.[94]

In this regard Peter Swire and Kenesa Ahmad concluded that three types of attackers can be distinguished. [95] First, the ''white hat'' hackers who are computer experts and make a living by detecting vulnerabilities and informing the public or users of encryption about the flaws in the system. Moreover, they could be the ''black hat'' hackers which include terrorists and criminals whose goal is to do harm, and the ''insider attackers'' who first helped to create the backdoor will secretly disclose the key. It does not necessarily have to be a criminal or terrorist who exploits the vulnerability. For example, it will not be the first time even corrupt police officers exploit the created vulnerabilities.[96] Moreover, the 2011 Wikileaks disclosures of enormous amounts of US governmental classified messages in 2011 was allegedly done by an insider. The illicit exploitation of vulnerabilities in security systems which caused harm to the public has also been illustrated in several cases. For example, in 2004 malicious users gained access to the Greek interception capabilities which were designed to be used by Greek law enforcement.[97] The phone calls of the Prime Minister and over one hundred other government officials were illegally intercepted. The perpetrators were never caught. Another example of flawed cryptography which resulted in exploitation of vulnerabilities by criminals are the Logjam and FREAK attacks, which compromised the Transport Layer Security protocols used to secure HTTPS connections worldwide. [98] Cryptography expert Susan Landau also considered the different risks of using backdoors. [99] As Landau states, backdoors which intend to facilitate interception of encrypted electronic communications can pose security problems that exceed the benefits received from the information collected.

Many scholars and organisations have pointed out the risk of exploitation. Bruce Schneier, a respected cryptographer, stated: ''I can design a secure system that has no backdoor access, meaning neither criminals nor foreign intelligence agencies nor

---

[93] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 433.
[94] Ronald L. Rivest, *''The Case against Regulating Encryption Technology''* (October 1998) p. 116-117.
[95] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 460-461.
[96] Cory Doctorow, ''Total corruption: Organised crime infiltrated and compromised UK courts, police, HMRC, Crown Prosecution Service, prisons, and juries'' (*BoingBoing*, 11 January 2014) <https://boingboing.net/2014/01/11/total-corruption-organised-cr.html> accessed 20 April 2018.
[97] Vassilis Prevelakis & Diomidis Spinellis, ''The Athens Affair'' (*IEEE Spectrum*, 29 July 2007) <https://spectrum.ieee.org/telecom/security/the-athens-affair> accessed 20 April 2018).
[98] David Adrian et al., ''Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice'' (Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Vol. 2015-October Association for Computing Machinery, 2015) p. 5-17.
[99] Susan Landau, ''Surveillance or Security? The Risks Posed by New Wiretapping Technologies'' (The MIT Press 2010).

domestic police can get at the data. Or I can design a system that has backdoor access, meaning they all can''.[100] It goes on by stating: ''Most of the time we recognize that harming the overwhelming number of honest people in society to try to /harm the few bad people is a dumb trade-off.'' The European Union Agency for Network and Information Security also considered the use of backdoors in encrypted communications, and considered the risk that vulnerabilities could be used by other people then law enforcement a main risk.[101] In the end, it takes a firm position by stating: ''The use of backdoors in cryptography is not a solution. Existing legitimate users are put at risk by the very existence of backdoors. The wrong people are punished.'' Furthermore, the EDRi stated that there is no consensus on who is liable in the case the bad guys take advantage of vulnerabilities and get access to data such as company secrets.[102] It is not a surprise that many computer scientists and cryptographers are strong opponents of backdoors because of the risk of exploitation by criminals and terrorists. In key escrow regimes this risk will even be more persuasive if there are multiple databanks or when many countries use such a regime. If keys are held in numerous places or countries, then there are many potential points of compromise. Peter Swire and Kenesa Ahmad stated that the ''independent'' databank might be coerced to hand over the keys to the local government, even in the absence of court orders or other rule of law protections. Consequently, important communications could come in the hands of the country you trust least in the world. [103]

In 1997, a group of leading computer scientists and cryptographers already published a comprehensive report on key escrow which is still relevant today.[104] They come up with three key escrow related risks, with their first one being the risk of exploitation by stating the high value of escrow databanks for criminals. [105] They might directly attack or corrupt insiders at the databank, effectively placing the keys in the hands of the bad guys. Moreover, communications to and from the databank also becomes a prime target for attackers when keys are being sent to this database. This transmission is also encrypted, but it has a single point of failure, namely the key of the recovery agent with which the transmitted keys are encrypted. If this key is compromised, all the keys which are encrypted using that key could be compromised.[106] In 2015, more or less the same group of computer scientists and cryptographers came up with an updated report stating that the ability of law enforcement to access all data and communications in today's

[100] Rob Price, ''Bruce Schneier: David Cameron's proposed encryption ban would destroy the internet'' (Business Insider, 6 July 2015) <http://www.businessinsider.com/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7?international=true&r=US&IR=T> accessed 20 April 2018.
[101] ENISA, ''*ENISA's Opinion Paper on Encryption. Strong Encryption Safeguards our Digital Identity''* (December 2016) p. 5.
[102] EDRi, ''Position paper on encryption. High-grade encryption is essential for our economy and our democratic freedoms'' (25 January 2016) p. 3.
[103] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 459.
[104] Hal Abelson; Ross Anderson; Steven Michael Bellovin; Josh Benaloh; Matt Blaze; Whitfield Diffie; John Gilmore; Peter G. Neumann; Ronald L. Rivest; Jeffrey I. Schiller; Bruce Schneier, 1997. *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, Columbia University Academic Commons.
[105] Ibid 11-12.
[106] Ibid 18.

complex, global information infrastructure will mandate insecurity.[107] First they mentioned a technical obstacle, namely that exceptional access to electronic communications would entail a U-turn from the best practices nowadays to improve secure communications.[108] The practice of forward secrecy which deletes decryption keys immediately after use and authenticated encryption could be an example. However, they continue with the risk of exploitation by the bad guys as well.[109] They give examples of exploitations by hostile actors in the past, such as the illicit exploitation of vulnerabilities in the Greek interception capabilities, and a similar case in India. As mentioned in Chapter 1, they also come up with several other questions such as the scope of applicability and supervision on backdoors. However, these are mere administrative questions on specifications of the system and are not relevant for the question to what extent backdoors are a proportionate solution.

This was just a small grasp of authors, but if one summarizes their arguments it all comes down to the same conclusion: a secure backdoor does not exist. As soon as a backdoor is created which allows access to encrypted communications, the bad guys will inevitably find and exploit it. According to EDRi, ''the answer to security problems like those created by terrorism cannot be the creation of security risks.''[110] Although law enforcement will use backdoors to safeguard national security and prevent crime, in reality this is just a false sense of security. However, the computer scientists and cryptographers do not come up with a solution to the problem of interception. This could be due to a clash of cultures. Computer scientists and cryptographers usually try to determine what is possible or not, while politicians and lawyers usually try to find a balance or compromise. This is inherent of their professions. Nevertheless, as we have seen in Chapter 1 even the Dutch government and European Institutions have understood this risk and therefore discourages the use of backdoors in encryption, since it would weaken the security of the system and the overall security of the country.

3.2.2 Complexities

The experts also highlighted in their 1997 report the inherent difficulty of building and maintaining a key escrow system.[111] Complexity is already a major challenge in developing encryption. A key escrow regime greatly multiplies this complexity, especially given the desire of law enforcement to access electronic communications within hours of transmittance.[112] According to the experts, key escrow will add enormous complications with security requirements unlike anything previously encountered in cryptography. The databank must first identify and authenticate the law enforcement agent, court order or other documentation, then authenticate the target user and data and checking for how long the communications must be intercepted. Subsequently, the key is recovered and the plaintext data is saved in a required format and securely transferred to the authorized parties, while maintaining an audit trail of

[107] Abelson et al., 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026.
[108] Ibid 12-13 and 18.
[109] Ibid 16-17.
[110] Maryant Fernández Pérez, ''EU's plans on encryption: What is needed?'' (*EDRi*, 16 October 2017) <https://edri.org/eus-plans-on-encryption-what-is-needed/> accessed 20 April 2018.
[111] Abelson et al., 1997. *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, Columbia University Academic Commons, p. 13-15.
[112] Ibid 15.

every step performed.[113] As already mentioned, each step is subject to possible attacks, such as through false law enforcement credentials or court orders. In their 2015 paper on backdoors, they repeat their concern by stating that it is impractical to store keys offline or to split it between different key escrow databanks, since fast access to the communications is highly preferred by law enforcement.[114] In the same report, they also state that the new technology which features access communications would have to be deployed and tested with ''literally hundreds of thousands of developers all around the world'' to be safe and secure.[115] Kocher, president and chief scientist of Cryptography Research placed this complexity in an international context.[116] He gives an example by stating that a Gmail sent to Japan from France by a laptop bought in Canada and made in China could be subject to decryption by law enforcement in five different countries. He concluded that technical challenges to create products that meet requirements of multiple laws would be a lot of work. In this regard, the group of cryptographers and computers scientists also asked in their 2015 report the question how timely approvals would be given for the millions of new products with communications capabilities when strong encryption is involved.[117]

3.2.3 Costs

In their 1997 report about key escrow the authors also mentioned that the development and maintenance of such a key escrow system could entails considerable costs.[118] These costs include the supervision of the databank, product design and substantial testing costs to assure the highest level of security, and costs for all the companies and other users who are required by law to comply with key escrow requirements. The deployment of a global key escrow infrastructure could potentially cost many billions of dollars.[119] The substantial costs are also mentioned in their 2015 report. [120] They conclude that when a key escrow regime is planned to be implemented, one should first thoroughly consider the many potential vulnerabilities and costs inherent to such a regime.

---

[113] Ibid.
[114] Abelson et al., 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026, p. 2.
[114] Ibid 12-13 and 18.
[115] Ibid 2.
[116] Tim Greene, ''Mandating backdoors for encrypted communications is a bad idea'' (*NetworkWorld*, 8 July 2015) <https://www.networkworld.com/article/2945374/security0/mandating-backdoors-for-encrypted-communications-is-a-bad-idea.html> accessed 20 April 2018.
[117] Abelson et al., 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026, p. 3.
[118] Abelson et al., 1997. *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, Columbia University Academic Commons, p. 16-18.
[119] Ibid 3.
[120]Abelson et al., 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026, p. 25.

3.2.4 Extraterritorial application

In their 2015 report on backdoors, the experts also mentioned another procedural obstacle, which would come down to a single question: who would control the escrowed keys?[121] Within the US, one could assume that the law enforcement or some other designated federal entity would hold the key in escrow and that judicial mechanisms would be constructed. Regarding independent third-party organisations, policymakers in the US already debated about the level of trust that could be placed in these databanks within the US border, considering its history of civil liberties and the rule of law. However, this leaves unanswered the question of what happens outside a nation's borders. Would encrypted data transmitted between the US and China need to have keys escrowed by both governments? Or could a single escrow databank be found that would be acceptable to both governments? And if so, would access be given to just one of the two governments or would both need to agree to a request? If this is the case, would Dutch, German or even Russian public and private organizations be willing to use messaging applications that gave the US government access to their data, especially when they could instead use locally built systems that do not? One must determine which countries have sufficient respect for the rule of law and are able to participate in an international exceptional access framework. How would such determinations be made? In this regard, Peter Swire and Kenesa Ahmad came up with the "least trusted country" concept , which is another example of how Internet security ''is only as strong as the weakest link.''[122] If country X demands backdoors, and someone is communicating electronically from country X to someone in country Y, then their communications can be intercepted when required regardless of their geographic location.[123] The least trusted country problem is essentially a thought experiment: how secure would India feel if Pakistan could also access the escrowed keys? In this situation, Indian's sensitive communications would be exposed to a country with which it has a violent history and a tough relationship. The same logic applies to whatever country a person trusts least, such as Israel and Iran, China and Taiwan, etc. It would be impossible to keep a backdoor solely for the use of e.g. the law enforcement in the US. [124] Once it exists, it will not be used for just one case. All law enforcement agencies in other countries will want access to the backdoor and will come up with similar demands.[125] Moreover, what if a developer in country X merely deploys a messing application, which is used by citizens in Country Y? Must it provide a vulnerability or

[121] Ibid 13.
[122] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 457.
[123] Ibid.
[124] Joseph Bonneau, ''A technical perspective on the Apple iPhone case'' (*EFF*, 19 February 2016) <https://www.eff.org/deeplinks/2016/02/technical perspective-apple-iphone-case> accessed 20 April 2018.
[125] Julia Powles and Enrique Chaparro, ''In the wake of Apple v FBI, we need to address some uncomfortable truths'' *The Guardian* (London, 29 March 2016) <https://www.theguardian.com/technology/2016/mar/29/apple-fbi-encryption-san-bernardino-uncomfortable-truths> accessed 20 April 2018.

provide the key to be escrowed to law enforcement in country Y?[126] Therefore, we cannot have a national solution to this. Any solution must be international.

As we have seen, what works well for internal corporate purposes or in a single jurisdiction simply cannot be applied to a global ecosystem of highly diverse technologies and legal systems.[127] Therefore, the EDRi stated that when the European Commission is defining its policy regarding backdoors, they should pay attention to the fact that the legal systems of the 28 EU Member States are very diverse and contain different safeguards for different challenging situations, and should note the current challenges to the rule of law in certain EU Member States.[128]

3.2.5 Avoidance

The European Union Agency for Network and Information Security stated that there is a high risk that criminals will develop and use their own cryptographic tools to communicate.[129] Kocher also considered this risk and stated that legal decryption of communications would force the bad guys to avoid using these communications. They would build their own, backdoor-free technology which would be readily available.[130] Peter Wood, an ethical hacker and member the ISACA London Security Advisory Group subsequently asks the question how banning encrypted communications such as end-to-end encryption is going to sort out criminals: ‘’Do they really think terrorists will think 'I'm not allowed to, so I won't use it’? The naivety astounds me."[131] The public-key encryption program called PGP (Pretty Good Privacy) is also widely available on the Internet. The rise of this software was one of the prominent reasons why the ‘’Crypto Wars’’ in the US ended in a loss for the government. As this PGP software spread, attempts to prevent the use of strong encryption became increasingly futile. Once PGP was easily downloaded from anywhere in the world, members of Congress and others increasingly realized that regulating encryption was not going to work.[132] Also the costumers who take privacy seriously might avoid software that has a backdoor in them. Banning backdoor free encryption in one country doesn’t stop someone just nipping across the border to install an app that is not banned and is not adhering to any national ban. Would Customs be required to impound the smartphones of tourists to check if they have encryption enabled? As stated in Chapter 1, for David Cameron's proposal to work, he will need to stop his inhabitants from installing software that comes from software developers who don’t comply and who are out of his jurisdiction. This is simply due because the law cannot be used to compel foreign firms to create

[126] Abelson et al., 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026, p. 3.
[127] Ibid 20.
[128] EDRi, *‘’Encryption Workarounds. A digital rights perspective’’* (12 September 2017) p. 5.
[129] Ibid 5.
[130] Tim Greene, ‘’Mandating backdoors for encrypted communications is a bad idea’’ *(NetworkWorld*, 8 July 2015) <https://www.networkworld.com/article/2945374/security0/mandating-backdoors-for-encrypted-communications-is-a-bad-idea.html> accessed 20 April 2018.
[131] Danny Palmer, ‘’Backdoors, encryption and internet surveillance: Which way now?’’ (*ZDNet*, 15 June 2017) <https://www.zdnet.com/article/backdoors-encryption-and-internet-surveillance-which-way-now/> accessed 20 April 2018.
[132] In 1999, there were over 200 co-sponsors of a bill to lift encryption export controls known as the Security and Freedom through Encryption (SAFE) Act, H.R. 850, 106th Cong. (1999).

vulnerabilities or create encryption keys[133] And if the software automatically chooses to which governments to comply using a technique such as IP geolocation, how does one prevent usage based on location spoofing?[134] Moreover, software which ensures secure communications are already free, widely available open source projects, maintained by thousands of independent programmers around the world.[135] Costumers who live in a complete different country and merely uses the software of a company that is obligated to have a backdoor according to some country's policy could also avoid the software. In this regard Kocher asks whether a potential corporate customer in Germany wants to buy encryption technology that the law enforcement in the US could defeat. Probably not.[136] Even companies that depend on strong security for their sensitive information and communications might relocate to another country. A country that stimulates the use of high end encryption strengthens its investment climate. Several companies have expressed highly negative views about the investment climate in the Netherlands in response to the recently proposed Security Act. For example, telecom company Voys said "If you value your customers' privacy, don't start up in the Netherlands''.[137]

3.3 Conclusion

This chapter first explained the rationale of backdoors in encrypted electronic communications. There is an increasing demand coming from law enforcements around the world that companies should be obligated to implement backdoors into their encryption, to make it possible for law enforcement to continue with the interception of electronic communications. This way, it will be more difficult for malicious parties to avoid detection and law enforcement will not miss out on evidence. When proposing the implementation of backdoors, one is talking about the intentional creating of vulnerabilities, of which the establishment of a "key escrow" regime is a well-known method. However, with the implementation of backdoors also comes with certain risks. Therefore, this chapter tried to summarize the most prominent risks that are known in academic literature and by other experts. As explained in detail, the risk of exploitation by malicious parties is discussed among the authors. When a vulnerability is created, anyone can take advantage of it, not just law enforcement. Sooner or later, a secret vulnerability will be exploited by a malicious user. Moreover, the development and maintenance of a key escrow regime is not easy to do. Complexity is inherent to such systems, especially given the desire of law enforcement to access electronic

---

[133] Ellen Nakashima and Barton Gellman, ''As encryption spreads, U.S. grapples with clash between privacy, security'' *The Washington Post* (Washington, 10 April 2015) <https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html?noredirect=on&utm_term=.bfbd4b8b31bd> accessed 20 April 2018.

[134] Abelson et al., 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026, p. 18-19.

[135] Cory Doctorow, ''David Cameron's internet surveillance plans rival Syria, Russia and Iran'' *The Guardian* (London, 13 January 2015) <https://www.theguardian.com/commentisfree/2015/jan/13/david-cameron-internet-surveillance-syria-russia-iran-communication> accessed 20 April 2018.

[136] Tim Greene, ''Mandating backdoors for encrypted communications is a bad idea'' *(NetworkWorld*, 8 July 2015) <https://www.networkworld.com/article/2945374/security0/mandating-backdoors-for-encrypted-communications-is-a-bad-idea.html> accessed 20 April 2018.

[137] Mark Vletter, ''Startups, stay away from The Netherlands if you value privacy'' (*Voys*, 29 July 2015) <https://www.voys.nl/weblog/startups-stay-away-from-the-netherlands-if-you-value-privacy/> accessed 20 April 2018.

communications within hours of transmittance. Such a system also comes with considerable costs, and could easily entail a clash between different jurisdictions. The answer to this clash must be an international solution. Which countries should have a key escrow databank, and how is this determined? In this regard the concept of the "least trusted country" is also discussed. Moreover, malicious parties could easily avoid using electronic communications with backdoors that are imposed by law by simply creating their own backdoor-free technology. Even costumers and companies themselves could avoid backdoors without too much of a hassle.

CHAPTER 4
ALTERNATIVES TO BACKDOORS

4.1 Purpose

This chapter will consider the alternatives that serve the same purpose as backdoors. As already mentioned in Chapter 1, this will mainly be done by using the taxonomy of encryption workarounds as described by Orin S. Kerr and Bruce Schneier, who specifically researched and categorised the workarounds of encryption.[138] However, their descriptions are kept short and again mainly focussed on device encryption. Nevertheless, they do come up with alternatives that can be used for intercepting encrypted electronic communications. Therefore, their taxonomy is a convenient basis to divide the different workarounds. Other alternatives that are kept outside of the taxonomy will also be discussed. This will make it clearer to understand if there are better solutions available rather than forcing companies to introduce backdoors in their encryption. First, the taxonomy of encryption workarounds is explained. Subsequently, two of these workarounds will be highlighted and other alternatives are discussed as well. In the end, the European Commission's anti-terrorism package for law enforcement will be critically reviewed. However, the existence of workarounds does not mean that law enforcement should use them nor that they would be necessary or proportionate, or even compatible with human rights law.

It should also be clear that mandatory key disclosure for encrypted communications already exists by law in several European countries if lawful interception of communications is not possible due to encryption.[139] Asking the suspect directly is not an ideal solution when performing covert surveillance. Moreover, most of the time this is even forbidden due to the privilege against self-incrimination. Therefore, companies or service providers can be compelled to disclose to law enforcement the decryption key that is used to encrypt electronic communications. However, this can only work up to a point where they have the key themselves. As we have seen in Chapter 1, this is often not the case. Other countries such as The Netherlands only have mandatory key disclosure to law enforcement regarding access to encrypted devices.[140]

4.2 A taxonomy of encryption workarounds

Orin S. Kerr & Bruce Schneier classified six kinds of workarounds that can bypass encryption schemes. The first three workarounds are key-based. The first way for the government to decrypt the data is to find an existing copy.[141] This copy must be stored somewhere, and law enforcement must be able to find and read it while having the lawful authority to do so. For example, the key can be stored on a USB drive or on a scratch of paper. A second workaround is guessing the key, by which law enforcement must correctly guess the key through e.g. brute force attacks.[142] The third workaround they mention is compelling the key from someone who has or knows it.[143] This person

[138] Orin S. Kerr and Bruce Schneier, Encryption Workarounds (March 20, 2017). Georgetown Law Journal, Forthcoming; GWU Law School Public Law Research Paper No. 2017-22; GWU Legal Studies Research Paper No. 2017-22.
[139] See regarding encrypted communications e.g., United Kingdom, Part III Regulation of Investigatory Powers Act (mandatory key disclosure), France, Law No. 2001-1062 (disclosure of encryption keys on authorization by a judge), and Spain, Law on Telecommunications 25/2007 (key disclosure).
[140] ''Automated works'', art 125k Code of Criminal Procedure.
[141] Orin S. Kerr and Bruce Schneier, Encryption Workarounds (March 20, 2017). Georgetown Law Journal, Forthcoming; GWU Law School Public Law Research Paper No. 2017-22; GWU Legal Studies Research Paper No. 2017-22, p. 996-997.
[142] Ibid 997-998.
[143] Ibid 1000-1001.

must be known and available to law enforcement and must be wanting to disclose the key. However, in some countries such a demand could be compelled through legal obligation. As one could probably notice, these three workarounds are mainly useful for device encryption. However, they could be used for encrypted communications, albeit in very limited circumstances. For example, when people communicate using Pretty Good Privacy software, they both hold a key which they might have stored, could be guessed or compelled. Nevertheless, in most cases when people communicate using widely available instant messaging applications or visiting HTTPS websites these workarounds are not very useful.

Orin S. Kerr & Bruce Schneier continue their paper with three non-key-based workarounds. The first workaround are backdoors which are already profoundly analysed in chapter 3. The second workaround is to access plaintext when the device is in use, because encrypted communications in transit must be decrypted in the end to be read on the screen of the recipient.[144] Therefore, law enforcement must have access to either the device of the sender or the recipient. This could be done by exploiting a vulnerability in the hardware of the device. This is something different than the exploitation of vulnerabilities in encryption algorithms as discussed in chapter 3.[145] This type of workaround is also known as hacking which requires the government to figure out a technical mean of gaining remote access to the device, which can raise complex legal questions. The third and final workaround is to locate a plaintext copy of the sought-after data.[146] Instead of bypassing encryption, it avoids encryption entirely. Again, this is mainly useful for device encryption rather than real time interception of electronic communications. However, there is one interesting detail that could be useful for this research. Law enforcement who wants to read e-mails or text might instead go to the cloud provider and see if copies of these communications are stored in the cloud.[147] However, to be successful, an available unencrypted copy of the data must exist. Moreover, law enforcement must have the legal authority to obtain the data and the unencrypted copy must be sufficiently up-to-date to be an adequate substitute of real time interception of communications. These workarounds correspond to EDRi's position paper on encryption workarounds, which used the taxonomy as laid down by Orin S. Kerr & Bruce Schneier as the basis for their work. [148] The last two workarounds, accessing plaintext when the device is in use and locating a plaintext copy of the sought-after data will be discussed further since these two are the most relevant workarounds for interception of electronic communications.

4.2.1 Hacking

Law enforcement can get covertly access to communications by exploiting a vulnerability in the hardware of a device or by secretly installing malware on the suspects device. Although the term 'hacking' is not used by law enforcement agencies, these practices essentially mirror the techniques used by hackers.[149] This technique is

[144] Ibid 1007-1008.
[145] Ibid 1008.
[146] Ibid 1010.
[147] Ibid.
[148] EDRi, *''Encryption Workarounds. A digital rights perspective''* (12 September 2017).
[149] Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, ''Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices'' (March 2017) p. 8.

already widely used by intelligence services, but also more and more law enforcements are hacking or are planning to. [150] Even end-to-end encryption does not matter anymore when one has control over the endpoint. Such a vulnerability or malware could entail a wide range of functionalities, such as making copies of the hard disk, keystroke logging, password interception, periodic screenshots and secretly turning on webcams or microphones. [151] Law enforcement might find these vulnerabilities themselves or through buying them. For example, they could buy exploits from the Italian Hacking Team company, which sells exploits to governments. This became publicly known because Hacking Team itself was hacked and lost their data including their zero days and costumer lists.

In 2016 the European Union Agency for Network and Information Security (ENISA) and Europol came with a Joint Statement, noting that the use of hacking techniques also brings several key risks.[152] The primary risk entails that hacking is much more intrusive then a backdoor, because it is in fact a backdoor in everything. It gives much more intrusive access than ever before and significantly restricts the fundamental right to privacy because devices nowadays store a lot of data. Through hacking, law enforcement can gain access to all stored data or data in transit from a device. Modern devices hold people's photos, video's, emails, messages, calendars, books, internet searches, as well as extremely sensitive data such as a person's location and movements, credit card information and passwords.[153] They can also be used to communicate with family members, including children. Each new form of communication is more intimate than the last. The Apple Watch can even let you transmit your heartbeat to your loved ones. This represents a significant amount of data as all their stored and communication in transit can be intercepted. A recent investigation by Dutch law enforcement collected seven terabytes of data, which translates into around 86 million pages of Microsoft Word documents.[154]

Moreover, governments who stash their vulnerabilities or participate in the zero-day market are exposed to major consequences, because these zero days will eventually leak out and will be used to attack our society which is increasingly dependent on technology.[155] For example, the WannaCry ransomware was a zero-day from the NSA and allegedly obtained by The Shadow Brokers, which leaked the ransomware to criminals.[156] Thus, governments are investing in finding zero-day exploits, but when they don't notify companies and citizens on time these exploits might get leaked and used to attack society. Therefore, Microsoft called in February 2017 for a Digital

[150] Ibid 10.
[151] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 462.
[152] ENISA and Europol, ''Joint Statement on lawful criminal investigation that respects 21st Century data protection'' (20 May 2016).
[153] Eoghan Casey and Benjamin Turnbull, ''Digital Evidence on Mobile Devices'' (3th edition, Elsevier 2011), p. 1-2.
[154] Openbaar Ministerie, ''Versleutelde berichten: schat aan criminele informatie'' (9 March 2017) <https://www.om.nl/actueel/nieuwsberichten/@98279/versleutelde/> accessed 20 April 2018.
[155] ENISA and Europol, ''Joint Statement on lawful criminal investigation that respects 21st Century data protection'' (20 May 2016).
[156] Samuel Gibbs, ''Shadow Brokers threaten to unleash more hacking tools'' *The Guardian* (London, 17 May 2017) <https://www.theguardian.com/technology/2017/may/17/hackers-shadow-brokers-threatens-issue-more-leaks-hacking-tools-ransomware> accessed 20 April 2018.

Geneva convention.[157] The current Convention says that you should not attack civilians, or bomb hospitals or schools in war time. Microsoft argued that in today's digital world we actually attack civilians even in peace time, because by looking for zero-day exploits and using these exploits the law enforcements risks that these might get out in the wild and are used against civilians in peace time. So, not even academics or NGO's, but even Microsoft complains that this approach with zero days will bring society into trouble.

The EDRi stated that law enforcement must be able to clearly explain why hacking is the least invasive option for getting protected information.[158] The necessity should be determined for every type of information that is obtained, and every user that is under surveillance. Mass hacking must be prohibited. Furthermore, governments should release reports at least annually on the acquisition and disclosure of vulnerabilities, and publish those that are discovered or purchased unless circumstances weigh heavily against disclosure. The EDRi concludes that they did not find any government who had put these principles fully in practice. Therefore, while the EDRi recognizes human rights-compliant government hacking as theoretically possible, all examples that they have seen in practice are inadequate to what is reasonably expected regarding safeguards.[159]

A study from the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Civil Liberties Justice and Home Affairs thoroughly compared the legal frameworks for hacking across several countries. It examined the legal and practical balances and safeguards implemented at national level to ensure the legality, legitimacy and necessity of restrictions to the fundamental right to privacy. It concluded that the EU Member States all do have certain safeguards in place. These safeguards include judicial authorisation of hacking practices, safeguards related to the nature, scope and duration of hacking such as restriction on the use of hacking tools based on the gravity of crimes, and independent oversight.[160] However, the study concludes with twelve additional concrete policy proposals and recommendations on hacking based on this comparative examination of the legal frameworks.[161]

4.2.2 Seizure of backups in the cloud

Law enforcement can also locate a plaintext copy of the sought-after data. Regarding interception of electronic communications, law enforcement might instead go to the cloud provider and see if backups of these communications are stored in the cloud. As already mentioned, an available unencrypted copy of the data must exist of which law enforcement must have the legal authority to obtain the data. It should also be noted that this workaround is only useful for interception of communications if these backups are up to date, to allow for (near) real time interception. WhatsApp already allows for

---

[157] Brad Smith, ''The need for a Digital Geneva Convention'' (Microsoft, 14 February 2017) <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> accessed 20 April 2018.
[158] EDRi, *''Encryption Workarounds. A digital rights perspective''* (12 September 2017) p. 9.
[159] Ibid 8-9.
[160] Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, ''Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices'' (March 2017) p. 10.
[161] Ibid 12-14.

automatic backups of your chats to Google Drive, and the frequency can be chosen.[162] Moreover, the same risk applies as to hacking. For example, most owners of Apple devices back up those devices to iCloud. If an iPhone user backs up an iPhone using iCloud, the online data can contain texts, notes, photos and videos, contacts, call history, calendar appointments and other information from the phone.[163] Even health data can be uploaded.[164] While not all data on a device is uploaded to the Cloud, many items are. Therefore, the seizure of a backup in the cloud also significantly restricts the fundamental right to privacy as there is a lot of data included in such a backup.

Apart from backups in the cloud, emails can also be directly seized from service providers. Emails are now typically encrypted using TLS, which means the message is encrypted between the user's computer and the service provider. For example, Google for Gmail, Microsoft for Outlook, etc. However, law enforcement can still acquire the content of these communications in plaintext, since most email providers store users emails for a certain period.[165] So, law enforcement could compel the email provider with a court order. A new UK surveillance law may require message service firms like Apple, Google, and Microsoft to honour such requests expeditiously and directly as a condition of doing business in the UK. In such cases, there must be uniform and transparent provisions for accessing communications, and for warrants or subpoenas.[166]

4.3 Mapping of metadata

The digital revolution has made more data about us available than ever before, and the government has more tools to obtain and analyse that data than ever before.[167] Therefore, according to David Kaye, governments have not demonstrated that the use of encryption by criminals or terrorists serves as an unbeatable barrier to law enforcement objectives.[168] A new report from the Berkman Center for Internet & Society at Harvard University confirms this as it states that law enforcement is actually not ''going dark'', because there are substantially amounts of other data available.[169] According to this report, one of the many reasons given for why the notion of "going dark" is far overblown is that even encrypted communications still generate metadata. For example, who communicated with whom, how often, for how long, using what network, etc. This is often more valuable to an investigation than the encrypted content itself. The difference worked in the wired phone days, but it no longer works. Therefore, one can argue that the distinction between intercepting content and metadata is increasingly

[162] WhatsApp, ''Backing up to Google Drive'' <https://faq.whatsapp.com/en/android/28000019/?category=5245251> accessed 21 April 2018.
[163] Apple, ''What does iCloud back up?'' (5 December 2017) < https://support.apple.com/en-us/HT207428> accessed 20 April 2018.
[164] Ibid.
[165] Most service providers are based in the US. In this regard, see 18 U.S.C. § 2702(a).
[166] Abelson et al., 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026, p. 19.
[167] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 466.
[168] OHCHR, ''Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye'', 22 May 2015, UN. Doc. A/HRC/29/32, p 14-15.
[169] Matt Olsen, Bruce Schneier and Jonathan Zittrain, ''Don't Panic. Making Progress on the "Going Dark" Debate'' (Berkman Center for Internet & Society at Harvard University, 1 February 2016).

difficult to draw and is less relevant, as metadata are now also privacy sensitive. Thus, another alternative to backdoors can be found: metadata mapping. [170]

There are two prominent types of metadata that are particularly relevant for law enforcement. First, location information is extremely useful for law enforcement. We are entering a new era in which most individuals carry a mobile phone which is connected to a wireless network and tracks your location. It is a standard feature, because the service provider needs to know where your phone is to forward calls to you.[171] The exact rules for storing location data vary by jurisdiction and service provider. However, in many jurisdictions location data is commonly stored for a significant period.[172] For example, providers in the US can be compelled by law enforcement to store such data, so that relevant location information can be preserved.[173] The number of such requests from US law enforcement has strongly increased in recent years.[174] However, during criminal activities location tracking can be avoided by using a simple prepaid phone or by refraining to use a mobile phone at all. Nevertheless, many people now carry and use mobile phones in their daily activities. Location information is thus available for surveillance purposes in historically new ways.[175]

Information about one's contacts is another prominent type of metadata that is particularly relevant for law enforcement.[176] In many criminal investigations, the identities of the parties involved could be as relevant as the content of the communications itself. The importance of social relationships has become especially famous through online social networks such as Facebook. For law enforcement, the mapping of a suspect's contacts is undoubtedly useful. The term "social graph" was conceived, to ''describe the global mapping of everybody and how they're related."[177] Therefore, social networking sites will also become a key focus in covert surveillance in the coming years. Peter Swire and Kenesa Ahmad came up with a list of relevant information in this regard, and concluded that wireline and wireless calls, e-mails, texts, VOIP communications, and social networking records contain a lot of useful information for law enforcement who are seeking information about a suspect's

[170] Upturn, ''What ISPs Can See. Clarifying the technical landscape of the broadband privacy debate'' (March 2016).
[171] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 467.
[172] Ibid.
[173] The retention periods are 90-day renewable periods, see 18 U.S.C. § 2703(f).
[174] ACLU, ''ACLU Seeks Details on Government Phone Tracking in Massive Nationwide Information Request'' (12 August 2011) <www.aclu.org/news/aclu-seeks-details-government-phone-tracking-massive-nationwide-information-request-0?redirect=technology-and-liberty/aclu-seeks-details-government-phone-tracking-massive-nationwide-information-0> accessed 20 April 2018.
[175] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 468.
[176] Ibid.
[177] Brad Fitzpatrick, ''Thoughts on the Social Graph, Bradfitz.com'' (17 August 2008) <http://bradfitz.com/social-graph-problem/> accessed 20 April 2018.

connections.[178] In the time of face-to-face communications, suspects would leave no trace of their connections. In today's world, if the suspect wants to prevent the government from gathering these data the suspect would need to hold back on many day-to-day activities. Those contacts will help law enforcement to additional targets of interest, while drawing a broader picture of the suspect itself

However, surveillance using metadata can constitute a serious privacy violation. Several EDRi members, Privacy International among them, have documented how damaging and overly extensive the use of metadata by law enforcement can be. [179] Nevertheless, many countries allow the collection of metadata much more often than content. As we have seen, metadata can help in key investigative tasks such identifying the location and establishing the existence of networks of individuals. The use of the internet has increased, and will continue to drastically increase, meaning that the amount of metadata available to law enforcement authorities will also drastically increase.

4.4 Other alternatives

Apart from the six workarounds as mentioned in Orin S. Kerr's & Bruce Schneier's paper and the mapping of metadata, there are other 'alternatives' thinkable that makes it possible for law enforcement to continue with their interception of encrypted electronic communications.

One example is a plain ban on encryption just like China and North Korea. However, encryption underpins everything we do on the internet, so such a ban would, for example, let criminals read your credit card details as you shop online and leave your digitised medical records open to all.[180] Therefore, a complete ban on the individual use of encryption technologies would disproportionately interfere with the freedom of expression, because it deprives all online users concerned of the right to create a private space for opinions and expressions.[181] Law enforcement could also use other forms of covert surveillance, such as infiltration or undercover operations. Although these examples could theoretically be alternatives on backdoors, it would not be convenient to have them as an alternative in the everyday interception of encrypted electronic communications. Therefore, this research will not further discuss these two alternatives.

[178] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 469.
[179] Privacy International, ''National Data Retention Laws since the CJEU's Tele-2/Watson Judgment. A Concerning State of Play for the Right to Privacy in Europe'' (September 2017).
[180] Bert-Jaap Koops, ''The Crypto Controversy: A Key Conflict in the Information Society'' (Kluwer Law International 1999), p. 131-132.
[181] OHCHR, ''Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye'', 22 May 2015, UN. Doc. A/HRC/29/32, p 14.

4.5 The European Commission's anti-terrorism package for law enforcement

The European Commission proposed in its anti-terrorism package inter alia technical and legal measures to support law enforcement to tackle the problem of encrypted communications.[182] It wants to do this without ''prohibiting, limiting or weakening encryption.'' As mentioned in Chapter 1, it is unclear what the Commission means when it stated that it was not proposing measures that could ''limit or weaken encryption", since this usually is the case when law enforcement is trying to bypass encryption. Therefore, it seems like the European Commission is struggling to find a position on encryption. [183] First, the Commission proposes a legal framework for cross-border access to electronic evidence. This research is not going to discuss cross-border access to electronic evidence, since the European Commission already came up with a framework in April 2018.[184] This framework merely deals with strictly cross border access to the evidence, blind if it is encrypted or not. Second, the Commission proposed six transparent measures to support Member State authorities.[185] However, these measures must be implemented with full respect of fundamental rights while also having the principle of proportionality in mind. This research will now discuss these measures one by one.[186]

- First, the Commission wants to support Europol to further develop its decryption capability. With regards to device encryption, an existing capability will be enhanced: when a Member State or law enforcement has an encrypted device obtained in a criminal investigation, Europol has an intelligent password guessing capability. This capability makes intelligent password guesses, rather than purely brute force attacks. Therefore, the authorities should ensure that they collect information on "possible passphrases, phrase fragments, character sets or password lengths" in investigative proceedings.[187] Subsequently they can unlock the device and obtain the evidence the court order entitles them to obtain from that device. According to the Council, the competent authorities should also investigate "weaknesses in algorithms and implementations" in order to take advertence of "possible errors" in encryption. Furthermore, in its report the

[182] Commission, ''Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union'' COM (2017) 608 final, p. 8.
[183] Joe McNamee, ''The European Commission struggles to find a position on encryption'' (*EDRi* 31 October 2017) < https://edri.org/european-commission-struggles-find-position-encryption/> accessed 16 April 2018.
[184] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD), and Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final - 2018/0107 (COD).
[185] Commission, ''Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union'' COM (2017) 608 final, p. 9.
[186] Graham Willmott also discussed these six measures in ''Caspar Bowden Political Panel, Encryption of Communications and E-evidence'' (Computers, Privacy and Data Protection Conference, Brussels, 26 January 2018).
[187] General Secretariat of the Council, The Council of the European Union, ''Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime" (Document no. 12711/17, 2 October 2017).

Commission states there will be 86 extra staff, however they corrected this later to zero.[188] What about encrypted electronic communications? The Commission does not go into that in this point, but one can only guess: the zero-day exploits as already mentioned in chapter 4. In January 2018 the Commission already announced it will invest 5 million euro in Europol's decryption platform to reinforce these powers.[189]

- Second, a network of points of expertise should be established. Many Member States are much more advanced than others. Therefore, sharing experiences and best practises is hopefully an easy win to bring some of the weaker capabilities up towards the capabilities of the stronger Member States.
- Third, Member States should have a toolbox of alternative investigation techniques, in which they bundle their best capabilities and practices. The network of points of expertise should contribute to developing this toolbox. However, the Commission is not clear what this ''magic toolbox'' will exactly entail. It would probably start with simple advices, for example if the police find a plugged-in device, it should not be unplugged. Or if it is unlocked, it should not be timed out to lock. Those might be basic practices to avoid mistakes during investigations. We'll have to see where the toolbox goes overtime. It may grow, but it will be a question of building confidence between Member State law enforcements.
- Fourth, there must be a structured dialogue with service providers and other industry partners.[190] If there is a structured collaboration between law enforcement and the industry, in which they sit down and discuss regularly what the issues are, what the concerns are and what is trying to be achieved, then they might find more practical steps to improve the objectives of law enforcement without challenging the interest of industry and privacy. However due to the inherent clash between parties, only very small and practical steps might come out of this collaboration. The Commissions also states they will promote "structured dialogue with industry and civil society organisations".[191] It is not clear what the Commission exactly wants, but the objectives might include convincing civil society organisations that strong encryption should not be enabled by default, making sure certain information other than message content is still observable, or otherwise changing software, hardware or protocols to suit law enforcements' needs.[192] Something along those lines seems to be happening

[188] Graham Willmott, ''Caspar Bowden Political Panel, Encryption of Communications and E-evidence'' (Computers, Privacy and Data Protection Conference, Brussels, 26 January 2018).
[189] Commission, ''Communication from the Commission to the European Parliament, the European Council and the Council, Thirteenth progress report towards an effective and genuine Security Union'' COM (2018) 46 final, p. 6.
[190] Commission, ''Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union'' COM (2017) 608 final, p. 10.
[191] European Commission, ''Questions & Answers: Security Union - Commission presents anti-terrorism package to better protect EU citizens'' (18 October 2017) <http://europa.eu/rapid/press-release_MEMO-17-3982_en.htm> accessed 20 April 2018).
[192] Matthijs R. Koot, ''EU Commission says it does not seek crypto backdoors, will propose legal framework in early 2018 for Member States to help each other access encrypted devices'' (19 October 2017) <https://blog.cyberwar.nl/2017/10/eu-commission-says-it-no-longer-seeks-crypto-backdoors-will-propose-legal-framework-for-member-states-to-help-each-other-access-encrypted-devices/> accessed 20 April 2018.

in the US as well. Nikki Floris, Deputy Assistant Director at the FBI, stated that ‘’The FBI is actively engaged with relevant stakeholders, including companies providing technological services, to educate them on the corrosive effects of the Going Dark challenge on both public safety and the rule of law, and with the academic community and technologists to work on technical solutions to this problem”.[193] However, as mentioned in Chapter 3, there is also a risk of avoidance by companies. If the UK government forces tech companies to stop using end-to-end encryption, then this might work for a UK-based company, but for international tech companies the UK is just one ordinary market among many. Even if the UK government managed to force the big players to conform, there would still be plenty of smaller players who would cheerfully refuse. Moreover, codes for encrypted messaging such as PGP is widely and freely available online and has been for decades. There are even more complicated technologies such as steganography that criminals can resort to if encryption is hampered. All this likely means any policy or legislation that comes out of the dialogue and hampers encryption will have to be evaluated thoroughly.

- Fifth are training programmes for law enforcement so they are better prepared to obtain encrypted communications. This speaks for itself. Development of relevant training courses given by CEPOL, the police training college.
- Finally, there is a need for continuous assessment of encryption technologies. Typically, law enforcement is playing catch up in these areas, since technical developments go fast. Therefore, the Commission is in favour of a function in Europol and perhaps in Eurojust to look up what technical developments are coming down the road and to inform law enforcements and policy makers.

In conclusion, these six measures are all worthy, but not world shattering nor surprising. Therefore, continuous reflection is needed in the era of encryption and to see what steps in the future are needed. The Commission will certainly be actively working on the implementation of these six measures for at least a decent period of time, but it is doubtful if it is enough for the coming years as the Commission themselves already stated that the use of encryption is expected to grow further in the coming years.[194]

4.6 Conclusion

This chapter used the taxonomy of workarounds as laid down by Orin S. Kerr & Bruce Schneier as a basis to distinguish different workarounds. In their report they came up with six different workarounds. The first three are key based: finding the key, guessing the key and compelling the key. The other three are non-key based: backdoors, accessing plaintext when the device is in use and locating a plaintext copy of the sought-after data. For this research, only the last two workarounds are particularly relevant to examine the workarounds in encrypted electronic communications. Accessing plaintext when the device is in use, or hacking, entails several risks, of which the intrusiveness and the risk of zero-day exploits being exploited by malicious parties

[193] Nikki Floris, ‘’Adapting to Defend the Homeland Against the Evolving International Terrorist Threat. Statement Before the Senate Homeland Security and Government Affairs Committee’’ (FBI, 6 December 2017) <https://www.fbi.gov/news/testimony/adapting-to-defend-the-homeland-against-the-evolving-international-terrorist-threat> accessed 20 April 2018.

[194] Commission, ‘’Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union’’ COM (2017) 608 final, p. 8.

are the most prominent ones. Therefore, the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs came up with twelve additional concrete policy proposals and recommendations on hacking based on their comparative examination of different legal framework. Locating a plaintext copy of the sought-after data, or in this case stored backups in the cloud, could be useful but again they are very intrusive since there is a lot of data included in such a backup, not only communications. Moreover, these communications need to be up to date to be a valuable encryption workaround in interception of communications. The digital revolution also made more data about us available than ever before, and the government has more tools to obtain and analyse these data. Location tracking and information about one's contacts are two prominent types of metadata that are extremely relevant for law enforcement. Nevertheless, surveillance using metadata also constitutes a serious privacy violation. Finally, the Commission came up with several legal and technical measures to support law enforcement in tackling the problem of encrypted communications. Although these measures are all worthy, none of them are really of vital importance in solving the problem of encryption. Therefore, it is doubtful if these measures are sufficient for the coming years as the Commission. In conclusion, there is no single magic way for the government to get around encryption. Different approaches will work in different kinds of cases and comes with different kinds of risks. There are no certainties about what will work. Although they do have one thing in common. These workarounds are extremely intrusive, since they do not merely give access to the communications, but to much more data of the suspect. Nevertheless, the law of encryption workarounds is still developing. Many workarounds raise complex and legal questions and courts are only at beginning of challenge those.[195]

[195] Orin S. Kerr and Bruce Schneier, Encryption Workarounds (March 20, 2017). Georgetown Law Journal, Forthcoming; GWU Law School Public Law Research Paper No. 2017-22; GWU Legal Studies Research Paper No. 2017-22, p. 1012.

CHAPTER 5
EVALUATION

5.1 The proportionality principle

This research used the doctrine as laid down by the ECtHR and academic literature to evaluate to what extent backdoors are a proportionate solution. In this regard, for a backdoor to be proportionate, it must be the least intrusive solution to the encryption problem and should not unduly infringe other fundamental rights. As mentioned, the implementation of key escrow entails several technical and legal risks:

- The risk of exploitation by malicious parties is discussed among many authors. When a vulnerability is created, anyone can take advantage of it, not just law enforcement. Sooner or later, a secret vulnerability will be exploited by a malicious user.
- The development and maintenance of a key escrow regime entails complexity. This is inherent to such systems, especially given the desire of law enforcement to access electronic communications within hours of transmittance.
- Such a system also comes with considerable costs such as the supervision of the databank, substantial testing costs, and costs for all the companies and other users who are required by law to comply with key escrow requirements.
- It could entail a clash between different jurisdictions. The answer to this clash must be an international solution and regaining trust in governments. Which countries should have a key escrow databank, and why?
- The malicious parties could easily avoid using electronic communications with backdoors that are imposed by law by simply creating their own backdoor-free technology. Even costumers and companies themselves could avoid backdoors without too much of a hassle.

However, these risks are inherent to basic government backdoor access requirements. [196] They exist regardless of the design of the escrow system, whether the databases are split with sharing techniques or maintained in a single hardened secure facility, and whether the databank provides the actual key or merely decrypts specific data as needed. As discussed in Chapter 4, the alternatives do not really have such technical and legal risks. On the other hand, they do significantly restrict the fundamental right to privacy:

- The three non-key based workarounds as discussed in Kerr & Schneier's paper are the least intrusive, however they are not relevant for this research. The other two non-key based workarounds are relevant but are the most intrusive of all.
    - Hacking is much more intrusive then a backdoor, because it is in fact a backdoor in everything. It gives much more intrusive access than ever before because devices store a lot of data nowadays. Through hacking, law enforcement can gain access to all stored data or data in transit from a device. This represents a significant amount of data as all their communication can be intercepted, as well as extremely sensitive data such as a person's location and movements. Moreover, just like backdoors, there is a risk of exploitation by malicious parties. Governments who stash their vulnerabilities or participate in the zero-

[196] Hal Abelson; Ross Anderson; Steven Michael Bellovin; Josh Benaloh; Matt Blaze; Whitfield Diffie; John Gilmore; Peter G. Neumann; Ronald L. Rivest; Jeffrey I. Schiller; Bruce Schneier, 1997. The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, Columbia University Academic Commons, p. 3.

day market can have their zero days leaked out which could be used to attack our society.
    - Law enforcement can also attempt to locate a backup of the suspects communications in the cloud. Again, if someone backs up his mobile phone in the cloud, the online data can contain much more data than merely the communications. Texts, photos and videos, notes, contacts, call history, health data and other information from the phone will be readily available for law enforcement. It should also be noted that this workaround is only useful for interception of communications if these backups are kept up to date.
- Mapping of metadata such as location tracking and gathering information about one's contacts are two prominent types of metadata that are extremely relevant for law enforcement. However, as mentioned several EDRi members have documented how damaging and overly extensive the use of metadata by law enforcement can be.

In other words, these alternatives on backdoors are extremely intrusive, since they collect much more data of the suspect then merely communications. Therefore, backdoors could be the least intrusive. For a backdoor to be proportionate it should not unduly infringe other fundamental rights as well. David Kaye already mentioned in its annual report on the promotion and protection of the right to freedom of opinion and expression that the freedom of expression is primarily at stake when backdoors are in force.[197] The same right that people have offline must also be protected online. However, a limitation of the freedom of expression is inherent to the intentional weakening of encryption. Whatever alternative the government uses to bypass encryption, it will limit the freedom of expression since the communications will be confiscated. This is also the case if the government collects metadata as an alternative to the content of communications.[198]

One can conclude that backdoors are indeed the least intrusive solution to the encryption problem and do not unduly infringe other fundamental rights. However, due to these legal and technical risks which are inherent to backdoors, it should not be wise to use backdoors as of now even though they are proportionate. If the brightest minds in the world cannot come up with something law enforcements want, someone should back down. One cannot just push ahead with something if it's not technically feasible. Therefore, one could argue that the issue of backdoors is not a case of privacy versus security, but rather a case of security versus security.[199] As we have seen, the computer scientists and cryptographers do not come up with a solution to the problem of interception. And even if hacking cannot be stopped, given the proposals around the world, we will need a much more stronger supervision then we ever had. Someone should watch over the guards, which will entail a huge problem in supervision. Not only by people with legal experience, but also technical experts who know what the risks and implications are of a certain exploit or malware. Nevertheless, a proper solution is

[197] OHCHR, ''Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye'', 22 May 2015, UN. Doc. A/HRC/29/32, p. 14-15.
[198] Ibid 19.
[199] Yochai Benkler, ''We cannot trust out government, so we must trust the technology'' *The Guardian* (London, 22 February 2016) <https://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi> accessed 21 April 2018.

needed given the increasingly use of encrypted communications worldwide. The more we rely on electronic devices to communicate with each other, the more likely it is that information that was once found in letters, will now be send in electronic form. Cryptography provides the electronic equivalent of letter covers, seals or rubber stamps and signatures.[200] However, it is also possible to intercept these under certain circumstances. According to Rod Rosenstein, Deputy Attorney General for the United States Department of Justice, the US ‘’has never had a system where evidence of criminal wrongdoing was totally impervious to detection, even when officers obtained a court-authorized warrant. But that's the world that is being created’’.[201] Therefore, compromises must be made to ensure that the law enforcement can continue to intercept electronic communications. The only solution would be a backdoor that takes away the technical and legal risks, but is still the least intrusive and does not unduly infringe other fundamental rights. As mentioned, these risks are inherent to basic government backdoor access requirements, but it does not exclude mitigation of these risks.

5.2 Mitigation of the risks

To mitigate the risk of exploitation by malicious parties, the key should be split between multiple databanks. This has its origins in the nuclear bunker where, to avoid the risk of a rogue actor launching a nuclear weapon, the government required two people, each holding part of a key, to put their parts together to unlock the weapon. As already mentioned in Chapter 3, the government wants (near) real time access to the data, which means the key must be readily available. Once law enforcement has gone through the security protocols, it can use the key to continue the interception of the suspect and real-time access is still possible. This way, the key that provides access can still be stored in highly secure databanks. Moreover, one can occasionally regenerate a new key for communications to limit this risk even further.

The fact that secure hard- and software engineering entails complexity is not relevant to question whether government access needs to be implemented. Therefore, this is not a valid argument against backdoors.[202] Complexity has not stopped society form developing complex systems before. One could even argue that our current state of technical innovation and development is based on our capacity to deal with the complexity of designing and maintaining increasingly advanced systems. Moreover, the internet with all its services is a global protocol that is working as well. Standardisation is crucial. Thus, it will only be a value if communication protocols will be harmonised. Most countries already share the view that interception must be standardised to achieve smooth cooperation between different law enforcements and ISP’s.[203] Moreover, international standards favour cryptosystems that have been proven to withstand

[200] ENISA, ‘*’On the free use of cryptographic tools for (self) protection of EU citizens’’* (20 January 2016) p. 1.
[201] CNBC, ‘’Exclusive: Department of Justice’s Rod Rosenstein Speaks at the Cambridge Cyber Summit Today’’ (*CNBC*, 4 October 2017) <https://www.cnbc.com/2017/10/04/exclusive-department-of-justices-rod-rosenstein-speaks-at-the-cambridge-cyber-summit-today.html> accessed 21 April 2018.
[202] Jaap-Henk Hoepman, ‘’The second crypto war is not about crypto’’ (8 December 2015) <http://blog.xot.nl/2015/12/08/the-second-crypto-war-is-not-about-crypto/> accessed 21 April 2018.
[203] Frost & Sullivan, *’’Lawful Interception: A Mounting Challenge for Service Providers and Governments’’* (16 May 2011) p. 2.

repeated attacks.[204] Therefore, it is crucial that the systems will be peer reviewed trough widespread and intense public testing before being implemented. As stated in this paragraph, the same could be said for considerable costs such as the supervision of the databank and testing costs.

With regards to the problem of extraterritorial application, I would like to refer to the US Department of Commerce's 90s proposal: envisioning a worldwide key management infrastructure with the use of key escrow and key recover encryption items.[205] Backdoors in communications will only be valuable if it is so widespread that it is used for most of the encrypted communications in different countries. Moreover, there must be high-availability, around-the-clock access to these communications. International standards should be considered in this regard. As we've seen in Chapter 1, countries including the UK, US and Australia are considering laws seeking government access to communications. If these world leading countries cooperate and come up with a global standardized system for government access, the jurisdiction problem would be mitigated already. However, different countries may have different legal requirements for interception. It would be hard to agree on certain standards if these differences are large or even conflicting. This is especially the case as the legal frameworks for government access in democratic societies is fundamentally different from such frameworks in a dictatorial regime. Furthermore, handing over the key to governments would require an extraordinary level of trust. After Edward Snowden's revelations the level of trust in governments collapsed.[206] It will only work if the level of trust is restored. Therefore, the keys should be handed over to agencies which are independent from the government.[207]

Global government access means that the use of encrypted communications must be highly regulated.[208] It would entail that the sale of un-escrowed products must be prohibited and the use of such products limited or banned to mitigate the risk that criminals are able to avoid key escrowed communications. Moreover, any information on how to patch or disable the key escrow regime in approved products must be prevented, as well as the source code that can be compiled to recreate the application. Nevertheless, it is imaginable that un-escrowed products that do not provide government access will be available to a small amount of people. As mentioned in Chapter 3, software such as PGP are widely available on the Internet. Such communications can only be prevented if all internet traffic is monitored and anything that looks like encrypted yet un-escrowed communications is blocked. This would be a preposterous task. However, 100% waterproof is not necessarily required. By

---

[204] Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157, p. 453.

[205] Dept. of Commerce, ''Interim Rule on Encryption Items," *Federal Register*, Vol. 61, p. 68572 (Dec. 30, 1996).

[206] Georgia Holmes and Sue Burum, *Apple v. FBI: Privacy vs. Security?*, National Social Science Journal, Volume 48 (2) 2016, p. 16.

[207] Nicole Perlroth, ''Security Experts Oppose Government Access to Encrypted *Communication'' The New York Times* (New York, 7 July 2015) <https://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html> accessed 21 April 2018.

[208] Jaap-Henk Hoepman, ''The second crypto war is not about crypto'' (8 December 2015) <http://blog.xot.nl/2015/12/08/the-second-crypto-war-is-not-about-crypto/> accessed 21 April 2018

sufficiently limiting the distribution and use of un-escrowed encrypted communications and making its usage a clear criminal offense, a substantial amount of people will simply not bother to use such communications. If criminals truly want to resort to these communications there is always a possibility. They could even resort to VPN's, which would conceal their identity from any prying eyes. However, in this case, other methods of surveillance would be more fitting.

5.3 A different approach

As mentioned, a backdoor is feasible especially if the risks of exploitation and the problem of extraterritorial application are mitigated. In this regard, I would like to refer to the ThinThread project of the NSA in the 1990s. There is little information about this project, but it was a system that could target and collect data in the case of a terrorist threat. [209] Bill Binney, one of the designers of the system, explained in an exclusive interview how the system worked.[210] It was a project that would gather metadata from fibre optic cables for the collection and raped analysis of billions of electronic records. It mapped out metadata to tag and categorise communications to eventually locate targets of interest based on metadata graphing techniques and social networking. These targets of interest would be analysed and refined for future collection of metadata. Encryption was used to protect all communications. When a specific target was found, a judge had to find probable cause to believe the target was involved in serious crimes. If this was the case, only then the data would get decrypted. Data from non-US citizens was ignored, unless it could be proven that this data was relevant for the investigation. According to Binney, it was ''a very disciplined, legal, constitutional acceptable process''. Moreover, because the system focused on targets of interest, less storage was needed than with the storage of unfiltered bulk communications. Nevertheless, the whole ThinThread project was cancelled by the NSA before it was adopted. According to Binney, the NSA rather chose for other projects that had less safeguards for privacy. However, this project is still relevant because it used metadata mapping to find targets of interest without bulk collection of data. Moreover, it enabled secure encryption for all communications. Unfortunately, the risk of exploitation and the problem of extraterritorial application would not be mitigated when his project would be implemented.

I would also like to refer to another project. David Chaum, one of the founding fathers of anonymity and encryption, came up with a similar idea with his PrivaTegrity project.[211] It is a network, designed to allow fully encrypted communications that no one can decrypt, whether it is law enfacement or a malicious party. It would be even more secure and efficient than existing online anonymity networks such as Tor or I2P. To be interceptable, it would entail a carefully controlled backdoor that allows anyone doing something "generally recognized as evil" to have their anonymity stripped. In

[209] Siobhan Gorman, ''NSA rejected system that sifted phone data legally'' The Baltimore Sun (Baltimore, 18 May 2006) <http://articles.baltimoresun.com/2006-05-18/news/0605180094_1_surveillance-national-security-agency-well-informed> accessed 21 April 2018.
[210] Fiona O'Cleirigh,''Bill Binney, the 'original' NSA whistleblower, on Snowden, 9/11 and illegal surveillance'' (*Computer Weekly*, April 2015) <https://www.computerweekly.com/feature/Interview-the-original-NSA-whistleblower> accessed 21 April 2018.
[211] Andy Greenberg, ''The father of online anonymity has a plan to end the crypto war'' (*Wired*, 1 June 2016) <https://www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/> accessed 21 April 2018.

ThinThread, this would've been done by mapping the metadata. For example, WhatsApp could stay encrypted, but it would have a backdoor for terrorism or child pornography. Just like in ThinThread, whoever controls the backdoor within PrivaTegrity would have the power to decide what counts as evil. In the case of ThinThread, it would have been the NSA and a judge. According to Chiam this is too much power for a single government. Therefore, he came up with an encryption protocol that sends encrypted messages through nine different computers in nine different countries that serve as intermediaries, each having a part of the key in escrow and stripping of a layer of encryption before it sends the text to the next computer.[212] A tenth server would serve as a ''manager'. This way, no single server, or even eight of the nine servers working together can decrypt the message. For the backdoor to work, nine server administrators in nine different countries would all need to cooperate to combine their data to reconstruct a message. Cooperation is key to trace criminals within the network and to decrypt their communications. Or as Chaum states: "It's like a backdoor with nine different padlocks on it.'' Chaum also suggests several safeguards, such as a limit on the frequency of covert interception and the reservation that communications could only be decrypted in the case of "serious abuse, something that leads to death and real harm to people or major economic malfeasance." Nevertheless, there is not much information available on this project as well and his project is still in development. The project also remains unclear on how these ''evil'' communications would be detected if all communications are encrypted.

Therefore, I propose we should come up with a ThinThread 2.0, combining the frameworks of both ThinThread and PrivaTegrity. Nine server administrators in nine different countries decide if the target is doing something generally recognized as evil. This could be based on mutually agreed policies. If this is the case, the communications are decrypted and interception can start. As mentioned, if law enforcement has gone through the security protocols, it can use the key to continue with real time interception. To detect what is found to be "generally recognized as evil", the framework of ThinThread steps in. This means mapping out metadata to tag and categorise communications to eventually locate targets of interest. These targets of interest would be analysed and refined for future collection of metadata. However, they will not be as profoundly scrutinized as described in Chapter 4, because a decryption order is possible. If a specific target is found and it is likely the communications contain evil content, it will be sent to the different administrators. What is important is that it solves both risks. First, the risk of exploitation by malicious parties is substantially mitigated. Spreading the keys among nine servers in nine countries makes it harder for hackers and corrupt government officials to exploit the backdoor. Moreover, the different server administrators will eventually develop their own security protocols for access, subsequently avoiding any single bug that could be used to enter all nine servers at once. To successfully exploit the backdoor, one must break all the different security protocols in all different countries. Second, the jurisdiction problem is lightened. The system already implies a cooperation between at least nine countries. It is an agreement on the rules of decryption of communications. The least trusted country problem is also mitigated, since you know at least nine countries are necessary to decrypt your communications. The order to decrypt would not be in the hand of a single company or

[212] David Chaum, Debajyoti Das, Farid Javani, Aniket Kate, Anna Krasnova, Joeri De Ruiter and Alan T. Sherman, cMix: Anonymization by high performance scalable mixing. Technical report, 2016, p. 2.

government. Instead you separate the key into pieces which are given to nine different countries. The only obstacle would be that the network must be implemented in already nine different countries to work and to cooperate in the network in finding evil communications. Which country should have a database? Therefore, I propose the EU should step in since all Member States pursue the same rule of law. It should not have to be international at first. The EU could also already come up with a design for the system or create a certain encryption algorithm that can be implemented in applications.

In any case, such a new system could be considered as one of the most ambitious and far-reaching technical projects of the information age. Therefore, more research is necessary to further develop this approach. There are still many procedural and administrative details lacking such as the range of systems to which such requirements would apply (public infrastructures, financial transactions, communications, etc) and whether certain anonymous communications would be allowed.[213] Nevertheless, what is important is that this approach would help law enforcement to intercept communications and protect society from terrorists and criminals, while at the same time respects people's privacy and protects their communications.

[213] For other questions, see Abelson et al., 2015. Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026, p. 20-24.

CHAPTER 6
CONCLUSION

To evaluate to what extent backdoors are a proportionate solution, this research used the doctrine as laid down by the ECtHR and academic literature. Accordingly, it attempted to examine if backdoors are the least intrusive solution to the problem that the use of encryption by criminals poses to law enforcement, as well as whether backdoors unduly infringe other fundamental rights.

To make this evaluation possible, it first explained the rationale of backdoors in encrypted electronic communications. As mentioned, there is an increasing demand coming from law enforcements around the world to bypass encryption in electronic communications. One often heard workaround would be the implementation of backdoors, which entails the intentional creation of vulnerabilities, of which the establishment of a key escrow regime is a well-known method. To further analyse backdoors, this research also examined the risks. The risks that are discussed are the risk of exploitation by malicious parties, the inherent complexity of backdoors, considerable costs, the problem of extraterritorial application and the avoidance of backdoors by criminals and terrorists.

This research also looked at the different alternatives that could bypass encryption. It used the taxonomy of workarounds as laid down by Orin S. Kerr & Bruce Schneier as a basis to distinguish the alternatives. In their report they came up with six different workarounds, however only the last two workarounds were particularly relevant. Accessing plaintext when the device is in use was the first one. As mentioned, this workaround also entails several risks, of which the intrusiveness and the risk of zero-day exploits being exploited by malicious parties are the most prominent ones. The second relevant workaround was to locate a plaintext copy of the sought-after data, or in this case stored backups in the cloud. Again, this is very intrusive since there is a lot of data included. Another alternative that is discussed is the mapping of metadata, but surveillance using metadata also constitutes a serious privacy violation. Finally, the Commission came up with several legal and technical measures to support law enforcement in tackling the problem of encrypted communications. Although these measures are all worthy, none of them were really of vital importance in solving the problem of encryption.

Finally, the framework of proportionality was applied on backdoors. The alternatives were extremely intrusive, since they collect much more data of the suspect then merely communications. Therefore, one could argue that backdoors are the least intrusive. Moreover, a backdoor does not unduly infringe other fundamental rights, since a limitation of the freedom of expression is inherent to the intentional weakening of encryption. Thus, one can conclude that backdoors are a real proportionate solution to the problem that the use of encryption by criminals poses to law enforcement, particularly as it relates to covert surveillance.

However, this is not a satisfying answer. Due to these legal and technical risks which are inherent to backdoors, it should not be feasible to implement them as of now. However, the mere fact that these risks exist does not mean that they cannot be mitigated. Therefore, a different approach is defined which tried to mitigate the risks of exploitation and the problem of extraterritorial application. Nevertheless, the mere mention of a "backdoor'', no matter how many padlocks and safeguards restrict it, is enough to send shivers down the spines of most computer scientists and cryptographers. The approach merely tried to debunk their arguments. It is not the perfect solution,

rather it is a bold attempt to end the impasse between surveillance and privacy activists. As made clear, encryption will even further increase in the coming years. Therefore, one can conclude that it is inevitable that compromises must be made, or else the government will indeed eventually lose the fight.

Bibliography

Books and journals

1. Abelson et al., 1997. The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, Columbia University Academic Commons.

2. Abelson et al., 2015. Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026

3. Bart van der Sloot, ‘’Ten Questions about Balancing’’ (2017) 3 (2) EDPL

4. Bart van der Sloot, ‘’The Practical and Theoretical Problems with ‘balancing’: Delfi, Coty and the Redundancy of the Human Rights Framework’’ (2016) 23 (3) Maastricht Journal of European and Comparative Law

5. Bert-Jaap Koops & Ronald Leenes, 'Code' and the Slow Erosion of Privacy, 12 Mich. Telecomm. & Tech. L. Rev. 115 (2005)

6. Bert-Jaap Koops, ‘’The Crypto Controversy: A Key Conflict in the Information Society’’ (Kluwer Law International 1999)

7. Bert-Jaap Koops, ‘’The Decryption Order and the Privilege Against Self-Incrimination. Do developments since 2000 suggest a need to force suspects to decrypt?’’ (Boom Lemma 2012)

8. Bert-Jaap Koops et al., A Typology of Privacy (March 24, 2016). University of Pennsylvania Journal of International Law 38(2): 483-575 (2017); Tilburg Law School Research Paper No. 09/2016

9. Brems, Eva and Lavrysen, Laurens, ‘Don't Use a Sledgehammer to Crack a Nut’: Less Restrictive Means in the Case Law of the European Court of Human Rights (January 2015). Human Rights Law Review 15 (1), 2015

10. Christopher Soghoian, Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era (August 17, 2009). 8 J. on Telecomm. and High Tech. L. 359; Berkman Center Research Publication No. 2009-07

11. David Adrian et al., ‘’Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice’’ (Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Vol. 2015-October Association for Computing Machinery, 2015

12. David Harris et al., ‘’Law of the European Convention on Human Rights’’ (3rd edition, Oxford University Press 2014)

13. De Hert, P. 2005. “Balancing Security and Liberty within the European Human Rights Framework. A Critical Reading of the Court’s Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies After 9/11.” Utrecht Law Review 1 (1)

14. Eoghan Casey and Benjamin Turnbull, ‘’Digital Evidence on Mobile Devices’’ (3th edition, Elsevier 2011)

15. Frost & Sullivan, ‘’Lawful Interception: A Mounting Challenge for Service Providers and Governments’’ (16 May 2011)

16. G. Lorenz, T. Moore, G. Manes, J. Hale and S. Shenoi, ‘’Securing SS7 Telecommunications Networks’’ (January 2001)

17. Georgia Holmes and Sue Burum, Apple v. FBI: Privacy vs. Security?, National Social Science Journal, Volume 48 (2) 2016

18. Gerald Chan. "Life after Vu: Manner of Computer Searches and Search Protocols. "The Supreme Court Law Review: Osgoode’s Annual Constitutional Cases Conference 67. (2014)

19. Gregory Coutros, 'The Implications of Creating an iPhone Backdoor.' (2016) 6(2) Nat'l Sec L Brief 81

20. James X. Dempsey, Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy, 8 Alb. L.J. Sci. & Tech. 65 (1997)

21. Matt Olsen, Bruce Schneier and Jonathan Zittrain, ‘’Don’t Panic. Making Progress on the “Going Dark” Debate’’ (Berkman Center for Internet & Society at Harvard University, 1 February 2016)

22. Michael Friedewald et al., ‘’Surveillance, Privacy and Security: Citizens’ Perspectives’’ (Routledge 2017)

23. Milaj, Jonida, *Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance*. In: International Review of Law, Computers & Technology. 2016; Vol. 30, No. 6

24. Nieuwenhuis et al., ‘’Hoofdstukken Grondenrechten’’ (3th edition, Ars Aequi Libri 2014)

25. Orin S. Kerr and Bruce Schneier, Encryption Workarounds (March 20, 2017). Georgetown Law Journal, Forthcoming; GWU Law School Public Law Research Paper No. 2017-22; GWU Legal Studies Research Paper No. 2017-22

26. S. Bortzmeyer, DNS Privacy Considerations, Internet Engineering Task Force, August 2015

27. Steven Greer, ‘’The exceptions to Articles 8 to 11 of the European Convention on Human Rights’’ (Council of Europe Publishing 1997)

28. Susan Landau, ‘’Surveillance or Security? The Risks Posed by New Wiretapping Technologies’’ (The MIT Press 2010)

29. Swire, Peter and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Columbia Science and Technology Law Review, Vol. 23, 2012; Ohio State Public Law Working Paper No. 157

30. Vlemminx, ‘’Het moderne EVRM’’ (Boom Juridsche Uitgevers 2013)

Reports

1. David Chaum, Debajyoti Das, Farid Javani, Aniket Kate, Anna Krasnova, Joeri De Ruiter and Alan T. Sherman, cMix: Anonymization by high performance scalable mixing. Technical report, 2016

2. EDRi, *‘’Encryption Workarounds. A digital rights perspective’’* (12 September 2017)

3. EDRi, ‘’Position paper on encryption. High-grade encryption is essential for our economy and our democratic freedoms’’ (25 January 2016)

4. ENISA, ‘*’’ENISA’s Opinion Paper on Encryption. Strong Encryption Safeguards our Digital Identity’’* (December 2016)

5. ENISA, ‘*’’On the free use of cryptographic tools for (self) protection of EU citizens’’* (20 January 2016)

6. ENISA and Europol, ‘’Joint Statement on lawful criminal investigation that respects 21st Century data protection’’ (20 May 2016)

7. FRA, *‘’Fundamental Rights Report 2017’’* (May 2017)

8. OHCHR, ‘’Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye’’, 22 May 2015, UN. Doc. A/HRC/29/32

9. OHCHR, ‘’Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci’’, 30 August 2016, UN. Doc. A/71/368

10. Privacy International, ‘’National Data Retention Laws since the CJEU’s Tele-2/Watson Judgment. A Concerning State of Play for the Right to Privacy in Europe’’ (September 2017)

11. Privacy International, ARTICLE 19 and IHRC, ‘*’Securing Safe Spaces Online. Encryption, online anonymity, and human rights’’* (17 June 2015)

12. Ronald L. Rivest, ‘*’The Case against Regulating Encryption Technology’’* (October 1998)

13. The Law Library of Congress, ‘’Government Access to Encrypted Communications’’ (*Global Legal Research Center* May 2016)

14. Upturn, ‘’What ISPs Can See. Clarifying the technical landscape of the broadband privacy debate’’ (March 2016)

Jurisprudence

1. Handyside v the United Kingdom App no 5493/72 (ECtHR, 7 December 1976)

2. Klass and Others v Germany App no 5029/71 (ECtHR, 6 September 1978)

3. Kruslin v France App no 11801/85 (ECtHR 24 April 1990)

4. Malone v the United Kingdom App no 8691/79 (ECtHR, 2 August 1994)

5. Z v Finland App no 22009/93 (ECtHR, 25 February 1997)

6. Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000)

7. Lee v the United Kingdom App no 25289/94 (ECtHR, 18 January 2001)

8. Slivenko v Latvia App no 48321/99 (ECtHR, 9 October 2003)

9. Segerstedt-Wiberg and Others v Sweden App no 62332/00 (ECtHR, 6 June 2006)

10. Weber and Saravia v Germany App no 54934/00 (ECtHR, 29 June 2006)

11. Üner v The Netherlands App no 46410/99 (ECtHR, 16 October 2006)

12. Kennedy v the United Kingdom App no 26839/05 (ECtHR, 18 August 2010)

13. Uzun v Germany App no 35623/05 (ECtHR 2 October 2010)

14. Supreme Court of the United States, Riley v. California, United States Reports 573 (2014)

15. Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015)

16. Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016)

Governmental documents

1. Art. 29 Working Party (2014), Opinion 05/2014 on Anonymization Techniques, WP 216, Brussels, 10 April 2014

2. Commission, ‘’Communication from the Commission to the European Parliament, the European Council and the Council, Eighth progress report towards an effective and genuine Security Union’’ COM (2017) 354 final

3. Commission, ‘’Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union’’ COM (2017) 608 final

4. Commission, ‘’Communication from the Commission to the European Parliament, the European Council and the Council, Thirteenth progress report towards an effective and genuine Security Union’’ COM (2018) 46 final

5. Dept. of Commerce, ‘’Interim Rule on Encryption Items," *Federal Register*, Vol. 61, p. 68572 (Dec. 30, 1996)

6. Directorate General for Internal Policies, Policy Department C: Citizens’ Rights and Constitutional Affairs, ‘’Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices’’ (March 2017)

7. Dutch Council of State. *Kamerstukken II* 2015/2016, 34 372, nr. 4

8. European Commission, ‘’Questions & Answers: Security Union - Commission presents anti-terrorism package to better protect EU citizens’’ (18 October 2017)

9. Explanatory Notes to the Act on the Intelligence and Security Services 2017

10. Explanatory Notes to the proposed Computer Crime III Bill

11. General Secretariat of the Council, The Council of the European Union, ‘’Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime" (Document no. 12711/17, 2 October 2017)

12. Information Commissioner’s Office, ‘’Encryption’’ (3 March 2016)

13. Letter from the Ministry of Security and Justice to the President of the House of Representatives of the State’s General. Cabinet’s view on encryption (01-2016) 26643-383

14. Openbaar Ministerie, ‘’Versleutelde berichten: schat aan criminele informatie’’ (9 March 2017)

15. People's Party for Freedom and Democracy (VVD), Christian Democratic Alliance (CDA), Democrats '66 (D66) and Christian Union (CU), ''Confidence in the Future: 2017-2021 Coalition Agreement'' (10 October 2017)

16. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD)

17. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final - 2018/0107 (COD)

18. Recommendation CM/Rec(2016)5 of the Committee of Ministers of the Council of Europe to member States on Internet Freedom, 13 April 2016

19. Statement by the Press Secretary, Office of the Press Secretary, The White House, ''The Clipper Chip Initiative'' (*EPIC*, 16 April 1993)

20. UN Human Rights Committee (HRC*), CCPR General Comment No. 27: Article 12 (Freedom of Movement*), 2 November 1999, CCPR/C/21/Rev.1/Add.9

Newspapers

1. Alex Hern, ''May calls again for tech firms to act on encrypted messaging'' *The Guardian* (London, 25 January 2018)

2. Andrew Sparrow, ''WhatsApp must be accessible to authorities, says Amber Rudd'' *The Guardian* (London, 26 March 2017)

3. BBC News, ''David Cameron says new online data laws needed'' *BBC News* (London, 12 January 2015)

4. Cory Doctorow, ''David Cameron's internet surveillance plans rival Syria, Russia and Iran'' *The Guardian* (London, 13 January 2015)

5. Ellen Nakashima and Barton Gellman, ''As encryption spreads, U.S. grapples with clash between privacy, security'' *The Washington Post* (Washington, 10 April 2015)

6. Julia Powles and Enrique Chaparro, ''In the wake of Apple v FBI, we need to address some uncomfortable truths'' *The Guardian* (London, 29 March 2016)

7. Nick Evershed, ''Australia's plan to force tech giants to give up encrypted messages may not add *up'' The Guardian* (London, 14 July 2017)

8. Nicole Perlroth, ''Security Experts Oppose Government Access to Encrypted *Communication'' The New York Times* (New York, 7 July 2015)

9. Samuel Gibbs, ‘’Shadow Brokers threaten to unleash more hacking tools’’ *The Guardian* (London, 17 May 2017)

10. Siobhan Gorman, ‘’NSA rejected system that sifted phone data legally’’ The Baltimore Sun (Baltimore, 18 May 2006)

11. Yochai Benkler, ‘’We cannot trust out government, so we must trust the technology’’ *The Guardian* (London, 22 February 2016)

Articles on websites

1. ACLU, ‘’ACLU Seeks Details on Government Phone Tracking in Massive Nationwide Information Request’’ (*ACLU*, 12 August 2011)

2. Andre Meister, ‘’Projekt „ANISKI“: Wie der BND mit 150 Millionen Euro Messenger wie WhatsApp entschlüsseln wil’’ (*Netzpolitik*, 29 November 2016)

3. Andy Greenberg, ‘’The father of online anonymity has a plan to end the crypto war’’ (*Wired*, 1 June 2016)

4. Brad Smith, ‘’The need for a Digital Geneva Convention’’ (*Microsoft*, 14 February 2017)

5. Chris Kanaracus & Steve Wilson, ‘’Expect renewed push for encryption backdoors from Trump administration’’ (*ZDNet*, 26 January 2017)

6. CNBC, ‘’Exclusive: Department of Justice’s Rod Rosenstein Speaks at the Cambridge Cyber Summit Today’’ (*CNBC*, 4 October 2017)

7. Cory Doctorow, ‘’Total corruption: Organised crime infiltrated and compromised UK courts, police, HMRC, Crown Prosecution Service, prisons, and juries’’ (*BoingBoing*, 11 January 2014)

8. Dan Froomkin & Jenna McLaughlin, ‘’FBI VS. Apple establishes a new phase of the Crypto Wars’’ (*The Intercept*, 26 February 2016)

9. Danny Palmer, ‘’Backdoors, encryption and internet surveillance: Which way now?’’ (*ZDNet*, 15 June 2017)

10. Fiona O'Cleirigh,’’Bill Binney, the ‘original’ NSA whistleblower, on Snowden, 9/11 and illegal surveillance’’ (*Computer Weekly*, April 2015)

11. Joe McNamee, ‘’The European Commission struggles to find a position on encryption’’ (*EDRi*, 31 October 2017)

12. Jordan Pearson & Justin Ling, ‘’Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages’’ (*Motherboard*, 14 April 2016)

13. Joseph Bonneau, ‘’A technical perspective on the Apple iPhone case’’ (*EFF*, 19 February 2016)

14. Kevin Bankston, ‘’Ending the Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors’’ (*Lawfare*, 14 June 2017)

15. Kim Zetter, “Hacker Lexicon: What is a Backdoor” (*Wired*, 11 December 2014)

16. Mark Vletter, ‘’Startups, stay away from The Netherlands if you value privacy’’ (*Voys*, 29 July 2015)

17. Maryant Fernández Pérez, ‘’EU’s plans on encryption: What is needed?’’ (EDRi, 16 October 2017)

18. Nikki Floris, ‘’Adapting to Defend the Homeland Against the Evolving International Terrorist Threat. Statement Before the Senate Homeland Security and Government Affairs Committee’’ (*FBI*, 6 December 2017)

19. Rob Price, ‘’Bruce Schneier: David Cameron's proposed encryption ban would destroy the internet’’ (*Business Insider*, 6 July 2015)

20. Serdar Yegulalp, ‘’Welcome to the era of encryption by default’’ (*InfoWorld*, 21 November 2013)

21. Tim Greene, ‘’Mandating backdoors for encrypted communications is a bad idea’’ (*NetworkWorld*, 8 July 2015)

22. Vassilis Prevelakis & Diomidis Spinellis, ‘’The Athens Affair’’ (*IEEE Spectrum*, 29 July 2007)

Other sources

1. Apple, ‘’New Version of iOS Includes Notification Center, iMessage, Newsstand, Twitter Integration Among 200 New Features’’ (6 June 2011) Press Release

2. Apple, ‘’This is how we protect your privacy’’

3. Apple, ‘’What does iCloud back up?’’ (5 December 2017)

4. Brad Fitzpatrick, ‘’Thoughts on the Social Graph, Bradfitz.com’’ (17 August 2008)

5. Europol ‘’Director’s speech at the Conference: privacy in the digital age of encryption and anonymity online’’ (19 May 2016) Press Release

6. Graham Willmott, ‘’Caspar Bowden Political Panel, Encryption of Communications and E-evidence’’ (Computers, Privacy and Data Protection Conference, Brussels, 26 January 2018)

7. Jaap-Henk Hoepman, ‘’The second crypto war is not about crypto’’ (8 December 2015)

8. Jay Stanley, ‘’Caspar Bowden Political Panel, Encryption of Communications and E-evidence’’

9. (Computers, Privacy and Data Protection Conference, Brussels, 26 January 2018)

10. Let’s Encrypt, ‘’Let’s Encrypt Stats’’

11. Matthijs R. Koot, ‘’EU Commission says it does not seek crypto backdoors, will propose legal framework in early 2018 for Member States to help each other access encrypted devices’’ (19 October 2017)

12. WhatsApp, ‘’End-to-end encryption’’

13. WhatsApp, ‘’Backing up to Google Drive’’

14. Yahoo, ‘*’Our Commitment to Protecting Your Information’’* (18 November 2013) Press Release