Sparkling Lights in the Going Dark:

Legal Safeguards for Law Enforcement's Encryption Circumvention Measures

*Thiago Moraes**

This article discusses legal safeguards that could be in place in the European jurisdictions when law enforcement authorities conducting investigations of criminal offenses implement circumvention measures to bypass encryption technologies designed to protect the right to privacy of users of electronic communication services and equipment. The analysis is structured in three parts: first, two encryption technologies used by communication applications and devices are explained: end-to-end encryption and full disk encryption. Second, two encryption circumvention measures are discussed: government hacking and unlock orders. This study discusses their effectiveness against those encryption techniques, as well as their degree of invasiveness and potential harm to individuals' rights to privacy and concludes with a list of possible legal safeguards that could be considered when implementing them. These safeguards are defined and discussed, based on European case law and national legislations analysis.[1]

Keywords: encryption; right to privacy; surveillance; going dark

I. Introduction

The 21st century has seen the rise of an information society that is continuously connected through the use of devices and networks. The development of communication tools has also increased the concern for privacy, since the potential for 'eavesdropping' a conversation became bigger. In order to avoid unwanted third party's interception, encryption mechanisms have been implemented in many telecommunication services that are widely used such as WhatsApp[2], Facebook Messenger[3] and Skype.[4]

However, encrypted communications are not used only by ordinary civilians: criminals, terrorists and other 'bad guys' also benefit from the use of these tools to avoid interception from law enforcement agencies. As better encryption mechanisms are developed and widespread, police and investigators raise their fear that efforts to gather evidence to prosecute and prevent crime are becoming more difficult and sometimes even impossible. In 2014, former US Federal Bureau of Intelligence (FBI) Director, Mr James Comey, gave a speech at Brooking Institution where he stated that the misalignment between law

DOI: 10.21552/edpl/2020/1/7

* Thiago Moraes, Master of Law and Technology from Tilburg University (Netherlands), a Master of Information Science and a Bachelor of Law and Network Engineering from the University of Brasilia (UnB); formely Blue Book Trainee at the European Data Protection Supervisor; co-founder of the Brazilian think tank Laboratory of Public Policy and Internet. For correspondence: <moraest@protonmail.com>.

1 This article is based on the thesis of this author submitted to the LLM in Law and Technology of Tilburg University in June 2019. For more in-depth information on the topic please see T Moraes, 'A Spark Of Light In The Going Dark: Legal Safeguards For Law Enforcement's Encryption Circumvention Measures' (Tilburg University 2019).

2 'WhatsApp FAQ - End-To-End Encryption' (WhatsApp.com) <https://faq.whatsapp.com/en/android/28030015/> accessed 10 January 2019.

3 'Secret Conversations | Facebook Help Centre | Facebook' (Facebook.com) <https://www.facebook.com/help/messenger-app/1084673321594605/> accessed 10 January 2019.

4 'Does Skype Use Encryption? | Skype Support' (Support.skype.com) <https://support.skype.com/en/faq/FA31/does-skype-use-encryption> accessed 10 January 2019.

and technology had created a public safety problem which he entitled as 'Going Dark'[5]. In short, Mr Comey argued that despite having the legal authority to intercept and access communications and information pursuant to court order, the FBI often lacked the technical ability to do so. Thus, he urged private and public sector to assist law enforcement agencies in dealing with this issue, by developing tools and legislations that circumvent encryption.

Although Mr Comey has become well-known for the use of the expression, he was not its pioneer since it was already being used by the academic community for quite some time. One such example is a paper by Swire and Ahmad, published in the spring of 2012, where the term is used and contrasted to the increase of surveillance power of public authorities, which by its turn is addressed as the 'Golden Age of Surveillance'.[6]

Even though the most inflated debates have happened in the US, with the FBI against big tech companies, (such as the battle against Apple's iPhone after the 2015 San Bernardino terrorist attack,[7] and more recently, in 2018, against Facebook's Messenger)[8], the discussion has also reached Europe, where many countries have implemented legislations to regulate encryption technology in communications. While the pioneer of these so-called anti-encryption provisions were the Netherlands, in 1993,[9] the United Kingdom has carried a big debate on the topic, not only in its first surveillance law, the Regulation of Investigatory Powers Act 2000 (RIPA), but also in the Investigatory Powers Act 2016 (IPA).[10] For example, RIPA allowed the UK government to compel private actors (companies and individuals) to give in their encrypted keys in situations where national security or the country's economic well-being were at stake.[11]

Other countries have also proposed legislations against encryption, although following a different approach, by giving the power to law enforcement authorities to bypass encrypted communications by hacking. Dutch national security agencies have the power to disable encryption of data, telecommunications, or data transfers and to install technical provisions in order to disable encryption of the data stored or transmitted in the computers they hack since 2002, and German authorities have been allowed to hack since 2004. France has also enacted a government hack legislation in 2011, although these powers have seldom been applied, due to the lack of resources and expertise of French authorities.[12]

This seems to go in straight opposition with the increasing concern on privacy, data protecting and security, and in the latter years many legislations have been approved covering these topics, with its most emblematic example being the EU General Data Protection Regulation (GDPR), which determines data security as one of its principles, and promotes encryption as an important measure to protect personal data in many of its provisions.[13]

As the debate heats up, the importance of finding a middle ground raise. Therefore, the research this article was based upon attempts to address the problem by answering the following question:

Which legal safeguards could be in place in the European jurisdictions when law enforcement authorities conducting investigations of criminal offences implement circumvention measures to bypass encryption technologies designed to protect the right to privacy of users of electronic communication services and equipment?

As a doctrine-legal type of research, literature on technical and legal content is explored, including academic papers, reports and website news. First, the

5 J Comey, 'Going Dark: Are Technology, Privacy, And Public Safety On a Collision Course?' (Federal Bureau of Investigation, 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> accessed 10 January 2019.

6 P Swire and K Ahmad, 'Encryption and Globalization' (Social Science Research Network 2011) SSRN Scholarly Paper ID 1960602, 463 <https://papers.ssrn.com/abstract=1960602> accessed 12 October 2018.

7 A Wainscott, 'A Golden Key to Pandora's Box: The Security Risks of Government-Mandated Backdoors to Encrypted Communications Notes' (2017) 44 Northern Kentucky Law Review 57, 68.

8 K McCarthy, 'ACLU: Here's How FBI Tried To Force Facebook To Wiretap Its Chat App. Judge: Oh No You Don't' (Theregister.co.uk, 2019) <https://www.theregister.co.uk/2019/02/13/facebook_fbi_messenger/> accessed 12 October 2019.

9 B-J Koops and E Kosta, 'Looking for Some Light through the Lens of 'cryptowar' History: Policy Options for Law Enforcement Authorities against 'going Dark'' (2018) 34 Computer Law & Security Review 894, 5 <https://www.sciencedirect.com/science/article/pii/S0267364918302413?via%3Dihub> accessed 12 October 2018.

10 B Acharya et al, 'Deciphering the Encryption Debate in Europe: United Kingdom' (Open Technology Institute 2017a) I <https://www.hoover.org/research/encryption-debate-europe> accessed 9 January 2019.

11 ibid 10.

12 B Acharya et al, 'Deciphering the Encryption Debate In Europe: France' (Open Technology Institute 2017b) II <https://www.hoover.org/research/encryption-debate-europe> accessed 11 January 2019.

13 As examples, see GDPR, arts 6(4), 32 and 34(3).

two main technologies used on electronic communications are identified and explained – end-to-end encryption (E2EE) and full-disk encryption (FDE). Second, two encryption circumvention measures are analysed – unlock orders, in which the government compel private actors to disclose the decryption key, and government hack.[14]

Finally, a list of legal safeguards is proposed. These were identified by a joint analysis of: (i) case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), and; (ii) national legislation assessment of four European countries, where encryption circumvention measures were implemented – UK, Germany, France and Netherlands.[15] These countries have been selected because they have been acknowledged for approving unlock order and/or government hacking legislations in the last years, as well as using malware during criminal investigations.[16] Furthermore, UK is a member of the UKUSA Agreement, a treaty for joint cooperation in signals intelligence, also known as the Five Eyes Agreement, which raises the attention of this country high interest on surveillance.[17] It must be stated that the assessment of these laws is in no way a comparative study, but an attempt to get more in-depth and identify other practices that have been proposed in these legislations.

The selected approach for identifying this set of safeguards has its limitations: since the safeguards come from multiple sources from different levels of jurisdiction, and there was no thorough analysis of their effectiveness, it should be clear that it was not possible to define which are the best and worst approaches. Therefore, the list presented is predominantly descriptive and does not necessarily represent an ideal approach to safeguards.

Encrypted data should not be confused with anonymised data. While encryption may be a technique to achieve anonymisation via randomisation, they are not synonymous and may have different goals.[18] Therefore, an encrypted data could only be considered anonymised if the decryption key would be destroyed, an operation that, for the sake of communications, would have no use.

While encrypted data for communications is still considered personal data, since this paper focuses in the context of criminal investigations, the relevant jurisdiction to be discussed will be the EU Directive 2016/680, also called the Law Enforcement Directive (LED).[19] Although the topic would also fall under the scope of the EU Directive 2002/58/EC,[20] the ePrivacy Directive, a thorough analysis of this legislation is avoided, since there is an advanced proposal for an ePrivacy Regulation,[21] which may include substantial changes to the current Directive. However, it must be stated that Article 5 of the ePrivacy Directive is explicit in addressing that the confidentiality of the communications should be ensured, even though there are exemptions for it, such as the prevention, investigation, detection and prosecution of criminal offences, as provided by Article 15(1).

Therefore, the analysis focus on the assessment of the conditions for interference on the right to privacy, as defined in the European Convention of Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (EU Charter). As it will be discussed, case law has provided for legal safeguards regarding surveillance measures but has not yet touched the topic of encryption circumvention, which has become a common practice of law enforcement operations. Furthermore, while literature on the topic has discussed some safeguards, they were never contrasted against existent case law or national legislations. Therefore, this text modestly discuss-

14 In the original research, three other measures are discussed with more in-depth: backdoor, key escrow systems and encryption banning legislations. See Moraes (n 1).

15 In the original research, Italy legislation was also assessed. However, the conclusion was that barely any safeguard was put in place, leading to its exclusion on this paper. See Moraes (n 1).

16 European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, 'Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices' (European Parliament 2017) <https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf> accessed 25 January 2019 18.

17 'National Security Agency | Central Security Service > News & Features > Declassified Documents > UKUSA' (Nsa.gov, 2019) <https://www.nsa.gov/news-features/declassified-documents/ukusa/> accessed 29 March 2019

18 Article 29 Working Party, 'Opinion 05/2014 On Anonymisation Techniques (WP 216)' (2014) 29 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 1 February 2020.

19 EU Directive 2016/680, regarding the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties [2016] OJ L 119/89.

20 Directive 2002/58/EC of the European Parliament and of the Council 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).

21 'Proposal For An Eprivacy Regulation - Digital Single Market - European Commission' (Digital Single Market - European Commission, 2020) <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation> accessed 1 February 2020.

es whether safeguards presented in case law on surveillance could be translated to the context of encryption circumvention, as well as identifies approaches of national legislators that could also be considered when developing a broader list of legal safeguards.

II. Encryption in Electronic Communication Services and Equipment

Before advancing to the legal issues regarding the regulation of cryptography in electronic communication services and equipment, it is important to define some building blocks. Therefore, some basics of the two common encryption technologies that have been continuously discussed in the battles of the Going Dark problem are herein discussed: end-to-end encryption and full disk encryption.

1. End-to-End Encryption

E2EE is used to provide confidentiality while data is being transmitted (data in transit). Many communication services, such as Instant Messaging (IM) and Voice over IP (VoIP) implement this solution: WhatsApp has introduced it on its messaging services in the end of 2014,[22] and Telegram, a competitor IM, has since its beginning offered E2EE, although not by default;[23] Skype, Microsoft's VoIP service, has started to offer E2EE in 2018, but also as an opt-in feature.[24]

In E2EE, a message is encrypted at its source and it cannot be decrypted until it reaches its final destination where it will be decrypted.[25] This means that neither Internet Service Providers, nor network devices (eg routers and repeaters) can access the plaintext or the decryption key. The same applies to the communication services intermediaries, such as WhatsApp, which does not store the private keys to decrypt the messages in its servers.[26] Besides IM and VoIP, two other applications that may use E2EE are electronic mail and file exchange.[27]

Many of these applications, such as WhatsApp, use an E2EE protocol designed in such a way that at no time its server has access to any of its clients' private keys.[28] This has caused difficulties to law enforcement agencies which, even when ordering warrants for the compulsory disclosure of keys, fail in their attempt, since companies do not hold them.

2. Full Disk Encryption

FDE is used to protect data stored in a physical device, such as a laptop or a smartphone (data at rest). The use of FDE by device manufacturers is not new: Apple first released FileVault, a disk encryption program for Mac computers in 2003.[29] However at the time, it was not implemented by default and most users did not care about setting it. However, in 2014, Apple introduced FDE in iPhone (iOS 8+) as a default solution.[30] Google followed up and start to implement FDE in Android devices running operating systems Lollipop 5.0 and above.[31]

Furthermore, FDE can be software-based or hardware-based.[32] The former occurs when it is performed in the operating system, and this research focus on this category, since the common struggle of law enforcement agencies is with smartphones' FDE solutions, that currently runs in the kernel-level. Most importantly, the decryption key is never sent to the

22 A Greenberg, 'WhatsApp Just Switched On End-To-End Encryption for Hundreds of Millions of Users' (WIRED, 2014) <https://www.wired.com/2014/11/whatsapp-encrypted-messaging/> accessed 23 January 2019.

23 'End-To-End Encryption, Secret Chats' (Core.telegram.org) <https://core.telegram.org/api/end-to-end> accessed 23 January 2019.

24 D Deahl, 'Skype Now Offers End-To-End Encrypted Conversations' (The Verge, 2019) <https://www.theverge.com/2018/8/20/17725226/skype-private-conversation-end-to-end-encrypted-opt-in> accessed 23 January 2019.

25 G Jacobson, 'The Public Key Muddle – How to Manage Transparent End-to-End Encryption in Organizations' (2015) Springer Fachmedien Wiesbaden 25, 26 <http://link.springer.com/10.1007/978-3-658-10934-9>.

26 WhatsApp, 'WhatsApp Encryption Overview' (WhatsApp 2017) <https://bit.ly/3a85CBc> accessed 23 January 2019 3.

27 Jacobson (n 25) 26.

28 J Lund, 'Signal partners with Microsoft to bring end-to-end encryption to Skype' (Signal.org, 2018) 4 <https://signal.org/blog/skype-partnership/> accessed 23 January 2019.

29 T Müller and FC Freiling, 'A Systematic Assessment of the Security of Full Disk Encryption' (2014) X Journal of Transactions on Dependable and Secure Computing 3.

30 Manhattan District Attorney's Office, 'Report Of The Manhattan District Attorney's Office On Smartphone Encryption And Public Safety' (2015) 1 <https://www.manhattanda.org/wp-content/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf> accessed 22 January 2019.

31 ibid 5.

32 Müller and Freiling (n 29) 1.

device and/or the operating system manufacturer, and stays stored in the user's device.

III. Law Enforcement Measures against Encryption

This section focuses on the discussion of two measures commonly used by law enforcement for encryption circumvention: government hacking, which is actually a group of techniques, sometimes presented as a compromise between taking no action and mandating encryption backdoors;[33] and unlock orders, that is, the request of judicial orders to compel the disclosure of keys by their holders.[34] It is important to understand that other measures also exist, as the heavily criticised backdoors, a vulnerability embedded in the code since its design, or yet, key escrow systems,[35] and legislative proposals for banning or controlling encryption.[36] However, due to the limits of this paper, they will not be covered here.[37]

1. Government Hacking

There are many different cryptanalysis techniques that can be used to access an encrypted plaintext. To give a glimpse, this paper will briefly talk about three of them, which have been known to be used by law enforcement authorities: brute-force, zero-day exploits and FDE-oriented attacks.[38]

a. Brute-Force Attacks

Brute-force attacks aim at breaking the cryptosystem by trying every possible key.[39] Kerr and Schneier refer to this as a 'guess the key' measure, and its usefulness will be determined by how fast the key can be found.[40] For a symmetric key, the difficulty of guessing it increases exponentially by each extra bit that is added to its length.[41] Even if it was assumed that a computing system could recover a DES key in a second, it would still take that same machine approximately 149 trillion years to crack a 128-bit AES key.[42] As already mentioned, some E2EE solutions, such as WhatsApp, use a 256-bit key.[43]

At first, brute-force seems to be more adequate to recover keys for data at rest. The reason is that devices such as smartphones often use passcodes to protect the keys, which are much shorter than the latter. Since the passcode unlocks the encryption key which, in turn, decrypts the encrypted data, guessing the passcode has the same effect as guessing the encryption key.[44] It would take an iPhone processor twenty-two hours to run through the one million possible keys under its default six-digit configuration.[45]

However, smartphone operational systems are designed with mechanisms to further difficult a brute-force attack: Apple's iOS 8+ implements as default escalating time delays for extra attempts,[46] and Android's 5+ requires a 30 seconds await after every 5 failed trials.[47] Furthermore, iOS can frustrate the whole attempt by turning on its wiping feature that deletes all data after 10 consecutive incorrect attempts.[48]In the San

33 Stiftung Neue Verantwortung, 'A Framework for Government Hacking in Criminal Investigations' (2018a) 6 <https://www.stiftung-nv.de/en/publication/framework-government-hacking-criminal-investigations> accessed 2 April 2019.

34 OS Kerr and B Schneier, 'Encryption Workarounds' (Social Science Research Network 2018) SSRN Scholarly Paper ID 2938033, 989 <https://papers.ssrn.com/abstract=2938033> accessed 12 October 2018.

35 H Abelson et al, 'The risks of key recovery, key escrow, and trusted third-party encryption' (1997) Columbia Academic Commons 5 <http://academiccommons.columbia.edu/catalog/ac:127127> accessed 15 February 2019.

36 In fact, that has been the case in some Northern African countries such as Tunisia, in favour of government surveillance. See UNESCO, 'Human Rights and Encryption' (UNESCO 2016) 48 <https://unesdoc.unesco.org/ark:/48223/ pf0000246527> accessed 15 February 2019.

37 For more details on these other measures, see Moraes (n 1).

38 Other techniques discussed in the original research are side-channel attacks and Internet of Things (IoT)-oriented attacks. See Moraes (n 1).

39 B Schneier, *Applied Cryptography* (2nd edn, Wiley 1996) 224.

40 Kerr and Schneier (n 34) 997.

41 Schneier (n 39) 225.

42 M Arora, 'How Secure Is AES Against Brute-Force Attacks?' *EE Times* (2012) <https://www.eetimes.com/document.asp?doc_id=1279619> accessed 18 February 2019.

43 WhatsApp, 'WhatsApp Encryption Overview' (WhatsApp 2017) 3 <https://bit.ly/3a85CBc> accessed 23 January 2019.

44 Kerr and Schneier (n 34) 998.

45 ibid 1000.

46 Apple, 'IoS Security: IoS 12.1' (2018) 15 <https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf> accessed 23 January 2019.

47 'Full-Disk Encryption | Android Open Source Project' (Android Open Source Project) <https:// source.android.com/security/encryption/full-disk> accessed 24 January 2019.

48 Apple (n 46) 15.

Bernardino case, the FBI pursued in court an order for the disabling of these anti-brute-force attacks features.[49] The agency claimed that once these features were disabled, the device could be easily hacked.

b. Zero-Day Exploits

Zero-day exploits are software codes that take advantage of zero-day vulnerabilities, which are bugs that create a security weakness in the design, implementation, or operation of a system for which no patch or fix has been publicly released.[50] Until the vulnerability is fixed, it can be exploited, enabling access to, monitoring, extracting information from, or damaging a software program. There are even markets for trade of zero-days, which are known to be used not only by criminals, but also by government agencies.[51]

One research conducted on zero-day vulnerabilities by the RAND Corporation concluded that exploits and their underlying vulnerabilities have a rather long average life expectancy of almost 7 years, and a low collision rate: the likelihood that a zero-day found by one entity will also be found independently by another in one year it is only 5.7%.[52] The researchers argued that these results may justify the high incentive for government agencies in stockpiling zero-days, but the non-zero collision rate may be reason enough for disclosing the vulnerability to the vendor and the public, avoiding exposing individuals to security risks.[53] However, ways of lowering government incentive to keep stockpiling remain to be discovered, since this is still mainly an ethical decision.[54]

c. FDE-Oriented Attacks

Many specific techniques can be used to circumvent Full Disk Encryption. First, there is Direct Memory Access (DMA), which aims to obtain the decryption key while it is stored in RAM. In order for it to work, the computer system must be powered on or in a suspend-to-RAM mode (a state where the CPU is powered off, but its context was swapped to the RAM).[55] Apple's iOS is said to be protected against this attack, by limiting external hardware access to the application processor memory.[56] A second type is Cold Boot attack, where the key is retrieved from RAM after rebooting a system. It relies on the remanence effect: low temperatures slow down the fading of a computer's memory content, and in the current technology, it can take as long as ten minutes to a complete disappearance, permitting an attacker to scan the memory for the key after the system has shut down.[57] Finally, there are Evil Maid attacks which basically consists of switching the device's master boot record (the hardware that contains information of a system start) with one that permit keystroke logging.[58]

As it may be noticed, one requirement of all FDE-oriented attacks is the physical access to the device (even if temporarily, in the case of Evil Maid).[59] At first, this may seem to be a hindrance, but law enforcement's powers to seize mobile devices or gather it as evidence from crime scenes are quite common.[60] A second issue may be the status of the phone: except for Evil Maid, the other types of attacks require that the device is turned on during apprehension. However, this seems also to be the case in real situations.[61]

2. Unlock Orders

Given the fact that law enforcement agencies may lack the resources and expertise to use hacking tools, and encryption banning legislations are heavily criticised, a recurrent approach has been the request of judicial orders to compel the disclosure of keys by their holders.[62] These keys may be held by either the device owner or by the companies who developed a

49 Manhattan District Attorney's Office (n 30) 21.

50 RAND Corporation, 'Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits' (RAND 2017) 2 <https://www.rand.org/pubs/research_reports/RR1751.html> accessed 19 February 2019.

51 M Fidler, 'Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2706199, 410 <https://ssrn.com/abstract=2706199> accessed 19 February 2019.

52 RAND Corporation (n 50) 51.

53 ibid 60.

54 Wainscott (n 7) 79.

55 Müller and Freiling (n 29) 4.

56 Apple (n 46) 41.

57 ibid 5.

58 ibid.

59 ibid 3.

60 Manhattan District Attorney's Office (n 30) 1.

61 Müller and Freiling (n 29) 8.

62 Kerr and Schneier (n 34) 989.

particular communication service or equipment, and each approach is criticized with different arguments.

Compelling assistance from the device owner raises many challenges, one of those being the privilege against self-incrimination, which is recognized within Europe.[63] The ECtHR has declared in *Saunders* that this privilege applies to right to remain silent, but not against the use of material compulsorily obtained which has an existence independent of the will of suspect.[64] However, it is still debatable how this rule applies to passwords disclosure: even if one may agrees that a password has an existence independent of the will of the suspect, it cannot be obtained independently from his will! Two other important cases may contribute to the non-disclosure of passwords by the suspect: in *Funke*, the ECtHR concluded that compelling a suspect to produce documents that law enforcement authorities believed to exist, without trying to procure the documents by other means was a breach of the right to a fair trial (Article 6 of the ECHR).[65] In *JB*, the Court stated that there can be no compulsory disclosure of documents and statement when there is no certainty that this information is held by the suspect, and any attempt to threaten him, such as fines and prosecutions, is by itself a breach of the right to a fair trial.[66]

Proving that the user knows the passcode may also be challenging: the defendant can always tell that she has forgotten the password, and the court may be unable to accurately determine if the defendant is testifying falsely or not.[67]Although a solution might exist when the user's device is protected by fingerprint, which is generally not protected by the privilege against self-discrimination, this feature is not set by default, and it is rarely turned on by devices' owners.[68]

A preferred approach to unlock orders are those targeted to companies that provide communication services (eg WhatsApp) or equipment (eg Apple). These orders may focus on the decryption of particular communications sessions or content, or the disclosure of the key necessary for the system's decryption. The latter is more criticised, since it could expose private data well beyond what should be required.[69]

The main debate here is how much authority the government has to force the private sector to assist in investigations, and under what conditions.[70] Sometimes, the encryption technology provided is designed in such a way that the key is not held by the companies, which is the case of E2EE and FDE technologies, as already discussed. In these scenarios, would the government have power to force these companies to create vulnerabilities to their own systems, such as backdoors?

To avoid suspicion from the target of surveillance, these orders often come with a prohibition for the industry to disclose information about the activity performed. These so called 'gag orders' are heavily criticised for not informing data subjects but also the general public about deliberate interferences with their rights, which hinders their rights to an effective judicial remedy.[71]

Another criticism against unlock orders is the undue burden they may create to tech companies.[72] In the *FBI v Apple* case, one of the arguments raised by the tech company in court was the burdensomeness of an assistance order seeking access to an iOS 8+ iPhone, because Apple would most likely have to develop new software or handover source code to the government in order to comply.[73]

IV. Legal Safeguards for Circumventing Encryption

1. The Right to Privacy

In Europe, the right to privacy is protected under Article 8 of the ECHR and Article 7 of the EU Charter as a positive right for private and family life, home

63 Koops and Kosta (n 9) 5.

64 *Saunders v the United Kingdom* App no 19187/91 (ECtHR, 17 December 1996).

65 *Funke v France* App no 10828/84 (ECtHR, 25 February 1993).

66 *JB v Switzerland* App no 31827/96 (ECtHR, 03 May 2001).

67 Kerr and Schneier (n 34) 1005.

68 K Jacobsen, 'Game of Phones, Data Isn't Coming: Modern Mobile Operating System Technology and Its Chilling Effect On Law Enforcement' [2016] SSRN Electronic Journal 582.

69 United Nations, 'Report of The Special Rapporteur On the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (2015) 15 <https://digitallibrary.un.org/record/1304394/?ln=en> accessed 18 February 2019.

70 Kerr and Schneier (n 34) 1015.

71 UNESCO (n 28) 57.

72 Jacobsen (n 68) 607.

73 J Potapchuk, 'A Second Bite at The Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data, Under The All Writs Act' [2016] SSRN Electronic Journal 1443.

and communications.[74] In the context of communications in the digital age, a common way to exercise the right to privacy has been the use of encryption.[75] In this sense, measures that aim to circumvent it, either by technical (ie government hacking) or legal means (ie unlock orders) are without any doubt an interference with the right to privacy.

According to Article 8(2) of the ECHR and Article 52(1) of the EU Charter, the right to privacy can only be legitimately curtailed by the government under certain conditions, which has given its status of a qualified right.[76] These conditions are quite similar in each one of these conventions. In the ECHR, it is stated that interference may occur if: (i) it is 'in accordance with the law'; (ii) it is for the pursuit of a 'legitimate interest' (such as national security, public safety or for the prevention of disorder or crime), and; (iii) it is 'necessary' in a democratic society. In the EU Charter the conditions for limitations requires that the interference to: (i) be 'provided by law'; (ii) respect the 'essence' of those rights and freedoms; (iii) be subject to the 'principle of proportionality' and; (iv) be 'necessary to meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others'.[77] Due to the limit of scope of this paper, these conditions will not be deeply discussed, but more in-depth can be found in the original research.[78]

However, it should be stated that the debate on encryption circumvention is closely related to the one on surveillance. In both situations, the right to privacy is interfered, and in many situations, the ECtHR and the CJEU have dealt with the surveillance of communications and telephone conversations. Therefore, it is important to highlight some decisions of these two European courts that translated the conditions for an interference with the right to privacy as a set of minimum safeguards that should be put in place. Even though these cases mostly refer to national security / intelligence operations, the safeguards developed by both Courts could also be considered to be put in place for law enforcement activities in the investigation of criminal offences, in particular when circumventing encryption. This can be reasoned from the fact that national security and criminal investigation activities use similar approaches and are both within the scope of surveillance.[79] Furthermore, encryption circumvention measures may be covered under a national surveillance regime, such as the case of the United Kingdom.

In this context, the ECtHR has developed a framework to determine the 'quality of law' in national legislations regarding surveillance mechanisms. First, it was presented in *Weber* a list of minimum safeguards that should be set out in to avoid abuses of power, which were mainly related with substantive and procedural aspects of the surveillance measures.[80] Later, in *Zakharov*, these safeguards were extended, to include rules regarding the accessibility of the law and oversight mechanisms.[81] In Table 1, the list of safeguards discussed in each case is shown.

As for the CJEU, surveillance measures were analysed in the context of data retention legislations, where the interference with Article 7 of the EU Charter was addressed. In *Digital Rights Ireland*,[82] the nature of offences and the categories of people targeted were considered.[83] It was also stated that substan-

74 In the UDHR and the ICCPR, the right to privacy is a negative right of no arbitrary interference with an individual's privacy, family, home or correspondence. These two aspects represent both sides of a same coin: the right to privacy gives autonomy for the individual in deciding how he is going to exercise it, but also set some limits for how this right can be interfered.

75 United Nations, 'The Right to Privacy in the Digital Age' (2014) para 1 <https://www.ifla.org/files/assets/faife/ochr_privacy_ifla.pdf > accessed 21 March 2019.

76 B van der Sloot, 'Where Is the Harm in A Privacy Violation? Calculating The Damages Afforded in Privacy Cases by The European Court of Human Rights' (2017) 8 JIPITEC 322, para 1.

77 A similar approach can be seen in other systems. The ACHR express that the restrictions for rights and freedoms may only be possible if: (i) 'in accordance with laws'; (ii) enacted for 'reasons of general interest', and (iii) 'in accordance with the purpose' for which such restrictions have been established. As for the ICCPR, it doesn't provide details of what should be an arbitrary or unlawful interference. However, the Office of the United Nations High Commissioner for Human Rights stated that in order for an interference with the right to privacy to be lawful, it should: (i) meet the 'principle of legality' (i.e. to be regulated by a legislation); (ii) be connected to a 'legitimate aim'; (iii) be 'necessary to achieve the aim' intended, and; (iv) 'proportional'.

78 Moraes (n 1).

79 European Parliament (n 16) 18.

80 *Weber and Saravia v Germany* App no 54934/00 (ECtHR, 29 June 2006) para 95.

81 Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015) para 231.

82 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] EU:C:2014:238.

83 According to the CJEU, the data retention measures should be restricted to (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences. See para 59 of the decision.

***Table 1**. Minimum safeguards in surveillance legislations, according to the ECtHR (Source: author)*

***Weber* (2006)**	***Zakharov* (2015)**
	Accessibility of law
Nature of offences	*Scope* of surveillance measures
Categories of people targeted	
Duration of surveillance measures	*Duration* of surveillance measures
Procedures: *examining, using* and *storing* the data	Procedures to be followed for *storing, accessing, examining, using,* communicating and destroying the intercepted data
Precautions when *communicating* the data to another parties	
Circumstances in which recordings may or must be erased or *destroyed*	
	Authorisation of surveillance (oversight 'before' the surveillance)
	Supervision of the implementation of surveillance (oversight 'during' the surveillance)
	Notification and *available remedies* (oversight 'after' the surveillance)

tive and procedural conditions should be in place, although no further details on that was given. Finally, it was highlighted the importance of prior review carried out by a court or by an independent administrative body when law enforcement authorities wish to assess the data retained.[84] The same safeguards were restated in *Tele2 Sverige and Watson*,[85] where the court reinforced that the authorisation regime must be followed up by a notification to the persons affected, as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities.[86] The CJEU also addressed that data should be retained in a 'particularly high level of protection and security by means of appropriate technical and organizational measures',[87] which is in some way related with the procedural safeguards of *Zakharov*. Therefore, all these safeguards have similarities with the ones developed by the ECtHR.

Regarding the scope of surveillance measures, both CJEU decisions declared that they should be limited to serious crimes, targeting only individuals that are likely to reveal a direct or indirect link to them.[88] However, this requirement was not considered in *Ministerio Fiscal*,[89] where the CJEU applied the principle of proportionality to affirm that 'non-serious' interference may be applied on 'non-serious' crimes. Although this decision could be subject to criticism, for the matters of this research, the understanding of the ECtHR as well as other practices applied by some national legislations and various soft law recommendations seem sufficient to conclude that the

84 C-293/12 and C-594/12 *Digital Rights Ireland* (n 82) para 62.

85 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] EU:C:2016:970.

86 ibid para 121.

87 ibid para 122.

88 C-293/12 and C-594/12 *Digital Rights Ireland* (n 82) para 62 and Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson* (n 85) para 111.

89 Case C-207/16 *Proceedings brought by Ministerio Fiscal* [2018] EU:C:2018:788.

limitation of surveillance measures to serious offences should be a minimum safeguard.[90]

2. Safeguards Implemented under National Legislations

As mentioned in the introduction of this paper, some European national legislations have introduced rules for encryption circumvention measures which may provide more in-depth to the set of minimum safeguards defined by case law. Therefore, four European countries have been selected (the reason for their choosing is explained in the introductory section): United Kingdom (UK), Germany (GE), France (FR) and Netherlands (NL).

a. United Kingdom

Two main regulatory acts cover the surveillance regime in the UK: Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA). The rules for unlock orders is covered in Part III of RIPA (power to require disclosure on the investigation of electronic data protected by encryption), while government hacking is under Part V of IPA (Equipment Interference). These rules are further explained by Codes of Practice that were published in 2018.

Section 49 of RIPA gives power to law enforcement agencies to issue *notices* requiring that protected electronic information which they have obtained (or are likely to obtain) lawfully be put into an intelligible form.[91] In order to be considered lawful, the notice has to follow a series of requirements, the first of which being to obtain appropriate permission. As a general rule, the authorisation should be granted by a judge. Necessity and proportionality tests should be addressed when granting permission.[92] Section 55 of RIPA requires some safeguards in the conducting of unlock orders and obtaining of the keys for protected information: data should be *retained in a secure manner* and all *keys should be destroyed as soon as no longer needed* and they are disclosed to the minimum number of persons necessary for the conducting of the investigation. For *oversight*, Section 65 of RIPA instituted the Investigatory Powers Tribunal (IPT), an independent judicial court with jurisdiction to consider complaints about surveillance. Although it has been criticised about its independency and impartiality, in *Big Brother Watch*, the ECtHR found no reasons to justify that the IPT violated the essence of the right to a fair trial.[93]

In what concerns government hacking, safeguards are provided by the IPA. Some of the safeguards in this legislation provide more in-depth to procedural safeguards defined as part of the minimum set in *Zakharov*, such as (i) the *security of data* and their deletion as soon as there is no longer any legal grounds for retaining it, meaning that data may need to be deleted even before the expiry of the warrant;[94] and (ii) the *prohibition on making unauthorised disclosures* of the data collected. [95]

Furthermore, the IPA provides some interesting safeguards that should be taken in account, since they may go beyond the minimum set of *Zakharov*. First of all, the *double-lock authorisation* mechanism, which has been considered a small step forward for the UK, when compared to the approach on traditional wiretaps: the hacking measure needs to be prior authorised by the law enforcement chief and a Judicial Commissioner (JC).[96] One probable advantage of this safeguard is to avoid enforcement agencies bias when authorising surveillance measures. For example, these agencies may have a different approach when applying the necessity and proportionality principle than an independent administrative or judicial body would have. A second best practice is the *publication of annual reports,* which contributes to transparency of the activities conducted under the surveillance regime.[97] Third, the requirement of *additional safeguards for items subject to legal privilege*, which gives an extra protection to certain categories of people.[98] Finally, the requirement of *further purpose limitation* for certain law enforcement agencies restricts the use of government hacking measures.[99]

90 For more on that see Moraes (n 1).

91 UK Government Home Office, 'Investigation of Protected Electronic Information Revised Code Of Practice' (2018a) 7.

92 ibid 36.

93 *Big Brother Watch and others v the United Kingdom* Apps nos 58170/13, 62322/14 and 24960/15 (ECtHR, 13 Sep 2018) paras 510-511.

94 IPA, s 129.

95 IPA, s 131.

96 Acharya et al (n 10) 9.

97 IPA, s 234.

98 IPA, s 132.

99 UK Government Home Office, 'Equipment Interference Code Of Practice' (2018b) 25.

b. Germany

Although Germany has no laws that force disclosure of encryption keys or decryption of content, it has an extensive legal regime to enable government hacking, which has been applied by both intelligence and law enforcement agencies.[100] The provisions that allow encryption circumvention in German law are spread over the Code of Criminal Procedure[101] (GCCP), the Federal Criminal Police Office Act[102] (FCPOA), the Telecommunications Act[103] and the Telecommunications Surveillance Directive.[104]

In the GCCP, §94, §98 and §100a provide rules that allows the circumvention of the security of an information system that has previously been seized through due lawful procedure, while §20k of the FCPOA allows the covertly hacking of information systems.[105] The legislation provides safeguards that should be considered before, during and after the measure is implemented. The ex-ante safeguards are as follows: (i) the target must be suspect of committing a *serious crime* or major offence;[106] (ii) the order must *target individuals*;[107] (iii) *a necessity test* should be applied;[108] (iv) only *essential changes* to the system are made, and they are *reversed* at the end of the measure; (v) *prior authorisation* from the judiciary is required, and in urgent cases, the court must confirm the order within three days.[109] In the case of covert surveillance, the order is limited to a maximum of three months, and *only one renewal* is allowed if the other conditions persist.[110] During the implementation, all the access and modifications should be registered.[111] Also, *data concerning the core area of the private life is regarded as off-limits and inadmissible*, and must therefore be deleted when accidentally accessed.[112]

As for ex-post considerations, the *persons affected* by a telecommunications interception order must be *notified* regardless of the use of the data collected in a criminal court case, as soon as it can be effected without endangering the investigation, persons involved or significant assets.[113] Also, every year, each *Länder* and the Federal Public Prosecutor General are required to submit a *report* to the Federal Office of Justice regarding the surveillance operations, which should include: i) the number of proceedings in which telecommunications interception measures were ordered; ii) the number of orders; and iii) the underlying criminal offence of the proceedings.[114]

c. France

Since 2015, the French Parliament has expanded the number of government hacking authorities and expanded penalties for failure to comply with unlock orders.[115] The French Code of Criminal Procedure[116] (FCCP) covers the rules for circumvention encryption both by unlock orders and government hacking measures. The former was introduced by Loi nº 2001 – 1062, while the latter by Loi nº 2016 – 731. The hacking provisions include the possibility for remote access to communication services and equipment.

While no safeguards could be found on the unlock order provisions, the rules for government hacking provide certain protections. First, there is need for *judicial authorisation*, which can come from two different figures: by the judge of freedoms and detention[117] in case of remote access initiated by the physical installation of software on a target computer;[118] and by an investigating judge for remote access to computer data, initiated remotely.[119] The measure can only be implemented in the pursuit of offences falling within the scope of Articles 706-73 and 706-73-1, which cover organized crime, terrorism and

100 B Acharya et al, 'Deciphering the Encryption Debate in Europe: Germany' (Open Technology Institute 2017c) III, 3 <https://www.hoover.org/research/encryption-debate-europe> accessed 11 January 2019.

101 In original, *Strafprozessordnung*.

102 In original, *Bundeskriminalamtgesetz*.

103 In original, *Telekommunikationsgesetz*.

104 In original, *Telekommunikations-Überwachungsverordnung*.

105 European Parliament (n 16) 78.

106 GCCP, §100a(1) and FCPOA, §20k(1). For the latter, covert hacking is only allowed if an assumption that a danger exists for (a) the body, life or freedom of a person or (b) threats which touches the 'foundations or the existence of the state' or the 'foundations of human existence' (eg national security).

107 ibid.

108 ibid.

109 GCCP, §100b (1).

110 FCPOA, §20k(6).

111 GCCP, §100a(6) and FCPOA, §20k(3).

112 GCCP, §100a(4) and FCPOA, §20k(7).

113 GCCP, §101.

114 GCCP, §100b(5) and (6).

115 Acharya et al (n 12) 2.

116 In original, *Code de Procédure Pénale*.

117 In original, *le juge des libertés et de la detention*.

118 FCCP, art 706-102-1.

119 FCCP, art 706-102-2.

other related *serious crimes*. The authorisation can be given for at maximum one month (if by the judge of freedoms and detention) or four months (if by the investigating judge), which can be renewed once.[120]

The safeguards presented in the French regime are directly related to the minimum set defined by European case law. However, some of those are worth being highlighted, as they can provide more in-depth to that set: (i) the *duty* for the examining magistrate or a commissioned judicial police officer *to maintain records of the operation; (ii) rules to avoid the retention of non-relevant data*; and (iii) the *deletion of data after the operation*.[121] Unfortunately, other safeguards related to the collection and use of data are only broadly provided in the general search and seizure provisions of the FCCP.[122]

d. Netherlands

Encryption circumvention measures in the Netherlands are also covered in its Code of Criminal Procedure[123] (DCCP). Rules for unlock orders and government hacking were both introduced in the DCCP by the Computer Crime Act, in 2018.[124] This reveals an increasing interest of this country on encryption circumvention measures.

Article 125k of the DCCP enables the investigating officer to order the decryption, or handing over of a decryption key or encrypted data.[125] This order is only to companies, since suspects are protected under the privilege against self-incrimination. The provision does not have specific safeguards on the matter, meaning that unlock orders are only protected by general procedural rules provided in the DCCP.

As for government hacking, Article 126nba provides the legal basis, and the safeguards for conducting it.[126] First, hacking can only be done if three conditions are met: it regards the investigation of *serious crimes*,[127] the crime constitutes serious breaches of law and hacking is urgently needed for the operation.[128] The order must be specific, *targeted to an individual*, and limited for a maximum of four weeks with possibility of a single renewal.[129] Also, *prior written authorisation* is needed from a judge, except in urgent cases, where it can be orally given by the magistrate, who has to write it down within three days.[130] The Explanatory Memorandum of the Computer Crime Act required the application of proportionality and subsidiarity tests when giving the permission.[131] The execution of the order is *supervised* by the Public Order and Safety Inspectorate.[132] If a zero-day vulnerability is used, its disclosure to the manufacturer can be delayed, as long as specific authorisation is obtained.[133] Finally, two ex-post safeguards are into place: (i) the *removal of any hacking tool after the investigation* has been completed, and;[134] (ii) the *notification of the targeted person* as soon as the interest of the investigation permits.[135]

3. Legal Safeguards

The joint analysis of European case law on surveillance measures together with the national legislations on encryption circumvention above mentioned allows to identify legal safeguards that could be in place when measures such as government hacking and unlock orders are put in place. These safeguards can be grouped in four categories: substantive, procedural, oversight and transparency.

a. Substantive Safeguards

Substantive safeguards are related with the limitation on scope and duration of the surveillance measures, as defined in *Zakharov* and *Tele2 Sverige and Watson*.

The limitations on scope should be based on the nature of the offence and the category of people targeted. The definition of what is a serious crime should be clear, but there is some flexibility of how

120 FCCP, art 706-102-3.

121 FCCP, art 706-102-7 to 706-102-9.

122 European Parliament (n 16) 74.

123 In original, *Wetboek van Strafvordering*.

124 In original, *Computercriminaliteit III*.

125 B-J Koops, 'Cybercrime Legislation in The Netherlands' (2010) 14.3 Electronic Journal of Comparative Law 10.

126 European Parliament (n 16) 90.

127 As described in art 67(1) of the DCCP.

128 DCCP, art 126nba(1).

129 DCCP, art 126nba(3).

130 DCCP, art 126nba(4) and (5).

131 European Parliament (n 16) 94.

132 In original, *Inspectie Openbare Orde en Veiligheid*. See DCCP, art 126nba(7).

133 DCCP, art 126ffa(3).

134 DCCP, art 126nba(6).

135 DCCP, art 126bb.

they should be defined: it can be presented as a specific list of crimes, or it may be related to the number of years of a maximum custodial sentence of the crime.[136] Furthermore, the legislation regarding encryption circumvention needs to state the specific condition where an individual or group of people should be targeted for the surveillance measure. An example is when one is suspected or accused of a serious criminal offence.[137] As a best practice, special protection should be in place in the occasion of privileged communication (eg between journalists and sources or attorneys and their clients).[138]

Duration should be proportionate to the common cycle of an investigation. Furthermore, the renewal should be possible only once. Finally, in the case of hacking, duration should be limited by removing the hacking tools after the end of the measure authorisation.[139]

b. Procedural Safeguards

In *Zakharov*, the ECtHR has established that the activities of storing, accessing, examining, using, communicating and destroying data should be clearly explained in the law and undergo a strict scrutiny.[140] After the implementation of an encryption circumvention measure, all data collected must be protected by procedural safeguards. A similar approach was taken in *Tele2 Sverige and Watson*, where the CJEU declares that appropriate technical and organizational measures should be implemented to ensure a high level of data protection.

Four procedural safeguards can be extracted from the case law and legislations analysed: (i) integrity and security of systems and their data; (ii) non-disclosure of data; (iii) deletion of non-relevant data and (iv) destruction of data after use. These procedural safeguards are related with principles on Article 4 of the Law Enforcement Directive: the two first with data security, the third with data minimisation and the third with storage limitation.

c. Oversight

The oversight mechanism is a safeguard that is required to guarantee that all other safeguards so far discussed are put in place, not only in the legislation, but also when implementing the interfering measure. All branches of government should be considered in the structuring of this oversight system.[141] In *Zakharov*, the ECtHR has stated that the oversight mechanism may come into play at three stages: when the surveillance is first ordered, while it is being carried out, and/or after it has been terminated.[142] By its turn, the CJEU declared in *Digital Rights Ireland*, that a review should be carried out by a court or by an independent administrative body when law enforcement authorities wish to assess retained data.[143] Therefore, five safeguards should be highlighted: (i) independent supervisory authority, (ii) authorisation regime (ie warrants); (iii) monitoring of the measure; (iv) notification; and (v) effective remedies.

As mentioned, in *Digital Rights Ireland*, the CJEU stated that an oversight regime should be conducted by an independent authority, either an administrative body or a judicial court. In order to avoid that judicial warrants resume to rubber-stamping, it is recommended a mixed model of administrative, judicial and/or parliamentary oversight, capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.

Warrantless measures should only happen in emergency situations such as when there is an 'imminent risk of danger to human life.' However, general purposes such as 'national security' or 'the prevention of disorder or crime' should not be considered as justifiable for a warrantless measure.[144] Also, in these urgent cases, authorisation should be subsequently obtained, and all data should be deleted and evidence suppressed if the supervisory authority concludes that the appropriate safeguards were not in place.[145]

Furthermore, as stated in *Zakharov*, intercepting agencies should keep records of the interceptions in order to that the supervisory body has effective ac-

136 European Parliament (n 16) 49.

137 *Roman Zakharov* (n 81) para 189.

138 Stiftung Neue Verantwortung (n 33) 17.

139 See *destruction of data after use*, in sub-s IV.2.d.

140 *Roman Zakharov* (n 81) para 231.

141 United Nations (n 75) para 37.

142 *Roman Zakharov* (n 81) para 233.

143 C-293/12 and C-594/12 *Digital Rights Ireland* (n 82) para 62.

144 J Lara, V Hernandez and K Rodriguez, 'International Principles On The Application Of Human Rights To Communications Surveillance And The Inter-American System For The Protection Of Human Rights' (2016) 19 <https://necessaryandproportionate.org/principles> accessed 2 April 2019.

145 European Parliament (n 16) 49.

cess to details of surveillance activities undertaken.[146] In this way, while the surveillance is being carried out, all the measures implemented, including the ones related to the circumvention of encryption should be registered in an independently verifiable audit trail, including any necessary additions, alterations or deletions of data.[147]

Notice that specific surveillance measures are in place is an essential requirement to guarantee access to effective remedies.[148] Without it, the individual might never be aware that surveillance was on her. To guarantee an appropriate balance between private and public interests, the ECtHR recommended that information should be provided to the persons concerned as soon as notification can be made without jeopardising the purpose of the surveillance.[149]

Only through the provision of an independent oversight body governed by sufficient due process and by being capable of ending ongoing violations that remedies can be deemed effective.[150] Besides ending ongoing violations, remedies should also counteract or make good any human rights harms that have occurred, by means such as apologies, restitution, rehabilitation, financial or non-financial compensation and punitive sanctions, as well as the prevention of harm through, injunctions or guarantees of non-repetition.[151]

In order to oversight to be truly effective, the sole reliance in the judicial system may not be enough. Therefore, alternative methods of surveillance control could be considered, such as quasi-judicial approaches, whose effectiveness has already been addressed by renowned scholars.[152]

d. Transparency

Although not explicitly mentioned in surveillance case law, transparency is closely related with oversight, since the latter requires that notices are provided to inform the individual about state surveillance of communications, their interception and the collection of her personal data.[153] However, the transparency requirement also refers to a broader level, by the publishing of periodical reports about the use and scope of communications surveillance techniques and powers.[154] When deciding what to publish, a suggested principle is the 'maximum disclosure', assuming that all their acts are public and can only be kept secret from the public under the strictest circumstances.[155]

In the context of unlock orders, citizens should be at least able to assess who issued the order, who gave authorisation and what information was shared. This approach is opposed to the so called 'gag orders', which prevent the industry not only from informing data subjects but also the general public about deliberate interferences with their rights.[156]

Within regards to government hacking, the transparency report should at minimum include the number of operations that have been conducted, the suspected crime, how many subjects with special protection were targeted, the percentage of targets informed, and what percentage of warrants were denied by the judiciary.[157] When zero-day vulnerabilities are used, the report should include information about how many were disclosed or retained, and if the latter, for how long.[158] Among the national legislations analysed, only the UK and Germany have implemented the obligation to publish periodic reports.

V. Conclusion

The Going Dark debate represents a continuous battle between public and private interests. Govern-

146 *Roman Zakharov* (n 81) para 233.

147 Privacy International, 'Government Hacking and Surveillance: 10 Necessary Safeguards' (2018) 29 <https://bit.ly/2J3LvYU> accessed 2 April 2019.

148 United Nations (n 75) para 40.

149 *Weber and Saravia v Germany* (n 80) para 135.

150 United Nations (n 75) para 41.

151 Privacy International (n 147) 42.

152 G Malgieri and P De Hert, 'European Human Rights, Criminal Surveillance, And Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably But Not Necessarily By Judges' [2017] Cambridge Handbook of Surveillance Law <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2948270> accessed 1 February 2020.

153 ibid 36.

154 United Nations, 'Report of the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2013) para 91 <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40> accessed 3 April 2019.

155 Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression, 'Freedom of Expression and the Internet' (2013) para 166 <http://www.oas.org/en/iachr/expression/docs/reports/ 2014_04_08_Internet_ENG%20_WEB.pdf> accessed 2 April 2019.

156 UNESCO (n 36) 56.

157 Stiftung Neue Verantwortung (n 33) 15.

158 Stiftung Neue Verantwortung, 'Governmental Vulnerability Assessment and Management' (2018b) 27 <https://www.stiftung-nv.de/en/publication/governmental-vulnerability-assessment-and-management> accessed 2 April 2019.

ments and theirs law enforcement agencies have at hands many different tools for circumventing encryption in communication applications and devices with the goal of preventing disorder or crime. Some of them can prove to be more or less harmful to individuals' fundamental rights to privacy and freedom of opinion and expression.

Although literature has criticised these measures and suggested some solutions, it could still be questioned which legal safeguards could be in place when law enforcement authorities conducting investigations of criminal offences implement circumvention measures to bypass encryption technologies designed to protect the right to privacy of users of electronic communication services and equipment. While measures such as backdoors, key escrow and encryption banning legislations should be avoided due to their bulk effect (ie they expose an indefinite number of individuals to mal-intentioned third-party attacks, and severely raise security risks), two measures may be more or less reasonable, as long as safeguards are put in place: government hacking and unlock orders.[159]

If the proper safeguards are not implemented, these two measures may still have a bulk effect. Thus the importance of limitation of scope and duration. Besides, government hacking tends to raise more security risks than unlock orders (since they might create vulnerabilities that can be explored by third-party attackers, such as zero-day exploits). However, the latter cannot bypass full disk encryption and end-to-end encryption, unless when implemented against the device's owner (who might be protected by the privilege against self-incrimination, or not even be known or be available). Since unlock orders are only a feasible solution when the decryption key is held by the service provider (ie cloud services or email), government hacking seems to be raising in adoption.[160]

Besides lessons from EU / CoE case law, it should also be considered that we can learn from Member States approaches. Some of the safeguards were only identified at national legislations, such as the double-lock authorisation regime of the UK's IPA, or the French approach of logging duties, obliging police investigators to maintain records of the operation, while avoiding the retention of non-relevant data; and deleting personal data after the operation. These safeguards can be interesting ways of reinforcing the protection of individuals' fundamental rights.

Finally, it must be stated that this paper is just one small spark in the continuous Going Dark debate. Many governments (both within and outside Europe) have raised their interest in encryption circumvention solutions (and surveillance, in general), putting several fundamental rights at stake. Besides the right to privacy, the rights to freedom of opinion and expression, to a fair trial and to effective remedies may be violated due to encryption circumvention measures.

Overall, the fact that governments have strengthened their surveillance powers in these last years may be preoccupying. If appropriate mechanisms to protect the right to privacy of individuals are not put in place, we may not be advancing to an era of Going Dark, but actually to the Golden Age of Surveillance.

159 In fact, this was one of the main findings of this paper: 'bulk effects' techniques should be avoided because they are a direct violation of the right to privacy. For more on that, see Moraes (n 1).

160 All these findings are better detailed in the original research.