The Dickson Poon
School of Law

Dissertation – 2019/20

Dissertation Module Code:	7FFLA903
Module Title:	LLM Dissertation, 60 Credit
Candidate Number:	A07222
LLM Pathway/Specialism:	LLM in Intellectual Property and Information Law
Dissertation Supervisor:	Perry Keller
Dissertation Title:	To what extent privacy and confidential communication breaches due to police surveillance on communication data in end-to-end encrypted instant messaging applications can be justified under the ECHR?
Submission Date:	01 September 2020
Word Count:	14,998

Acknowledgement

I would like to thank the Republic of Turkey Ministry of Education for their financial assistance and funding during my master's degree and their support during the COVID-19 period. Without those supports, I could not complete the master's degree.

Furthermore, I also would like to thank the Information and Communication Technologies Authority of Turkey ("BTK") for following my master's degree process closely and for their support during my dissertation period.

Table of Contents

Abstract

This dissertation discusses should law enforcement authorities be able to monitor individuals' communication data from end-to-end encrypted instant messaging applications and how surveillance should be done under the ECHR. First, it will examine the right to communication confidentiality and applicability of instant messaging applications to Article 8 ECHR. Followed by the significance of providing privacy and security within those applications and the place of the end-to-end encrypted system; the hardships of law enforcement authorities on communication data surveillance on end-to-end encrypted instant messaging applications and possible solutions will be analysed. Then, surveillance on both content data and metadata will be discussed separately. Finally, how to monitor metadata will be examined.

1. Introduction

Confidential communication is viewed as one of the most controversial issues in today's world. While enabling people to exercise their freedom of expression effectively, it is alleged that it can cause a danger to the prevention of crimes and national security. Moreover, with the innovations in communication tools, privacy concerns have become more complicated. Communication tools such as instant messaging applications started to use high-security methods to enable confidentiality. Therefore, it became disputable whether confidential communication in the digital era poses a threat to national security and the prevention of crime.

Both people and law try to shape themselves according to technology, but it is getting hard to keep up with its speed. The priorities of people, the matters they value, and how much time they spent to do something are changing day by day. For instance, whilst people in different cities could communicate with each other with letters which take days or months, nowadays it takes shorter than second thanks to instant messaging ("IM") technologies.

IM applications have become highly popular due to their ease of use and amazing features. Then, to provide communication confidentiality, IM applications have started to use end-to-end encryption.[1] In this way, communication content on those applications cannot be accessed by anyone except the sender and the receiver of the message.[2] Thus, the security of individuals' data which has become one of the most valuable possessions in the world is provided.

Needless to say, this effective protection was not welcomed by law enforcement authorities. Due to the end-to-end encrypted ('E2EE') IM applications such as WhatsApp, law enforcement authorities have started not to get any information they want to get.[3] With the encryption method that these applications use, lawful interception of the content of communication has become nearly impossible.

Governments and law enforcement authorities mostly argue that E2EE IM applications provide a safe place for criminals or terrorists to escape from authorities, then raise serious concerns about national security.[4] So that those applications should be prohibited, or a back door should be provided

---

[1] WhatsApp, 'WhatsApp Encryption Overview Technical White Paper' (*WhatsApp*, 2016) <https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf> accessed 19 June 2020

[2] Ibid

[3] Federal bureau of investigation, 'Going Dark' (Federal Bureau Of Investigation's website, 2016) <https://www.fbi.gov/services/operational-technology/going-dark> accessed 01.06.2020

[4] Nicholas Watt, Rowena Mason and Ian Traynor, 'David Cameron pledges anti-terror law for internet after Paris attacks' The Guardian (Brussels, 12 January 2015)

for the authorities. Nonetheless, privacy supporters claim that such moves are neither necessary in a democratic society nor proportionate.[5] Thus, the privacy of individuals and the confidential communication should also be considered. Then, authorities should not be allowed to get access to E2EE IM applications' content data. Balancing these is an extremely hard problem and presents strong debates.

This dissertation will investigate to what extent law enforcement authorities should be allowed for surveillance on communication data from E2EE IM applications under the European Court of Human Rights ("the ECtHR" or "the Court") perspective. In the first two sections, whether E2EE IM applications are protected under Article 8 of the European Convention on Human Rights ("the ECHR" or "the Convention") will be examined. To do this, initially, an overall introduction will be given to the right to communication confidentiality. Following the examination of IM applications under this right with the "living-instrument" approach of the Court, the importance of the privacy within those applications and end-to-end encryption will be analysed.

The next section will try to answer the question of which kind of communication data may be monitored by law enforcement authorities during surveillance on E2EE IM applications by referring to the issues of "going dark" and "back doors" and the separation between content data and metadata.

In the last part, how law enforcement authorities can monitor communication metadata of E2EE IM applications in light of the ECtHR decisions. The surveillance on communication data will be analysed according to requirements of "in accordance with the law", "necessity", and "legitimate aim".

2. Applicability of Article 8 ECHR in Instant Messaging Applications

The next part will discuss whether communication made via IM applications is considered confidential and whether it is protected within the scope of Article 8 ECHR. To do this, first, the right to communication confidentiality, the right to privacy, and the right to data protection will be touched. Then, while discussing the concept of the "living instrument" of the ECHR, the place of the IM applications within the right to communication confidentiality will be analysed.

[5] Nidhi Rastogi, WhatsApp Security and Role of Metadata in Preserving Privacy. in Bryant and others (eds), Proceedings of the 12th international conference on cyber warfare and security (Academic Conferences and Publishing International Limited 2017) 269

2.1 Confidential Communication as a Fundamental Right

Communication is a basic social function that is important for people to express themselves and to participate in social environments. Hence, communication is the basic nature of human life.[6] As stressed under Article 10 ECHR, everyone has the freedom "*to hold opinions and receive and impart information and ideas without interference by public authority and regardless of frontiers.*" As can be seen from the wording of the article, people should be able to both hold and share information, namely, communicate as a necessity of a democratic society.

Communication can be regarded as a tool to share information. In this context, it is necessary to explain the concept of information. Information is a highly sensitive term as it forms a basis for both privacy and communication, particularly in the digital era. As Purtova mentioned: "*Everything is or at least contains information*".[7] However, the law does not value every information equally. Indeed, that value depends on the effect of information on freedoms, fundamental rights, and interests of people. If a piece of information relates to an individual's "inviolate personality", that relationship between the information and the individual must be guarded with a right, which is called 'right to privacy' as first determined by Warren and Brandeis in 1890.[8] Legal arrangements were also quick after the beginning of literature studies on privacy. In 1948, the United Nations has published the Declaration of Human Rights referring to the right to privacy.[9] Only two years later, the Convention has also regulated the right to privacy with nearly identical words. As stated by Article 8 of the ECHR: "Everyone has the right to respect for his private and family life, his home and his correspondence."[10] In other words, everyone has their own area which others must be prohibited to interfere.[11] For these reasons, the information should be protected due to its connection with individuals' privacy.

Individuals' private and family life, their homes, and their correspondences are protected with the right to privacy. This means that unauthorized access to individuals' private life is prohibited. At the same time, Article 8 ECHR stresses that communication between people is also private and should be confidential thereby using the term "correspondence". Similarly, the right to respect private and family life has been laid down under Article 7 of the Charter of Fundamental Rights of the European

---

[6] William Mciver and others, 'The Internet and the right to communicate' [2003] 8(12) First Monday <https://doi.org/10.5210/fm.v8i12.1102> accessed 19 June 2020

[7] Purtova Nadezhda, 'The law of everything Broad concept of personal data and future of EU data protection law' [2018] 10(1) Law, Innovation and Technology 40-81

[8] Samuel Warren and Louis Brandeis, 'The Right to Privacy' [1890] 4(5) Harvard Law Review 193-220

[9] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 5

[10] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8

[11] Lawrance Lessig, Code: Version 2.0 (2nd edn, New York: Basic Books 2006) 201-210

Union ("the Charter") as "Everyone has the right to respect for his or her private and family life, home and communications".[12] Unlike the Convention, the Charter has modernised the provision and used the term "communications" instead of the term "correspondence". Even though their wordings are different, it can be said that their meanings are nearly identical within the interpretation of the ECtHR discussed above. In that way, both the Convention and the Charter provide individuals with the right to communication confidentiality.

The right to communication confidentiality and the right to privacy has been considered under the same right. Nonetheless, as the context of the term privacy has been extremely changed due to the conveniences with which technology provides governments and businesses the right to privacy has begun to be unable to offer sufficient protection to confidential information.[13] Far less protection of privacy was needed before because privacy existed in circumstances, at home, or in the belongings of people. However, technologies began to erode that circumstantial privacy. Technologies drew private matters out into the public, and it started with postal communications, then telegraph and telephone, and finally the internet.[14]

After these explanations, the right to data protection should also be mentioned in this context. The right to privacy does not compass information that is not private to an individual. [15] However, if a piece of information is not private, but it relates to an identifiable person, such information should also be protected.[16] This data is protected by the right to data protection. First, the right to data protection has been referred to in the OECD Guidelines.[17] Then, the right to data protection has been regulated via Convention 108 which is also binding for several non-member countries of the Council of Europe.[18] However, the Data Protection Law is mainly regulated by European Law. Initially, the EU Data Protection Directive has been implemented to protect personal data.[19] Then, it was replaced with

[12] Charter of Fundamental Rights of the European Union [2000] OJ 1 364/1 art 7
[13] Perry Keller, 'The Reconstruction of Privacy through Law: A Strategy of Diminishing Expectations' [2019] 9(3) International Data Privacy Law 132-152
[14] Ibid.
[15] Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' [2013] 3(4) International Data Privacy Law 222-228
[16] Ibid
[17] Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58/FINAL]
[18] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981 European Treaty Series No 108)
[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ 2 281/31

the General Data Protection Regulation ("GDPR").[20] Similarly, for policing purposes, Law Enforcement Directive ("LED") has been regulated.[21] According to the GDPR, personal data is defined as "*any information relating to identified or identifiable natural person*".[22] Therefore, even though a piece of data is not private to a data subject, it is still protected under the right to data protection.

The term "private life" in the provision must be interpreted broadly.[23] The ECtHR states that personal data is also covered by the expression of the private life, provided that there is an extra factor such as systematic collection and storage of information.[24] As the term personal data is broadly explained, any information may fall within the scope of personal data, so do communication data that is taken from IM applications. As discussed, the right to communication confidentiality has a discrete extent since separate elements are protected via this right than the right to privacy or the right to data protection.[25] Thanks to these developments and regulations, communication confidentiality is regarded as a separate fundamental right.

Confidential communication via IM applications is a fundamental right of individuals. While individuals using these applications, a huge amount of data is created so that the issue of confidential communication relates to more than one fundamental right. Since IM applications cause communication data to be processed, the right to data protection applies to this concept. Then, as confidentiality is necessary for communication to provide individuals with effective freedom of expression and freedom of assembly and association, those freedoms are also playing an effective role in confidentiality. However, more importantly, the right to communication confidentiality can be regarded as an umbrella combining all those rights and freedoms.

---

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 119/1

[21] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ 2 119/89

[22] General Data Protection Regulation art 4

[23] Kokott and Sobotta (n 15)

[24] Rotaru v Romania App no 28341/95 (ECHR, 2000)

[25] Frederic Zuiderveen Borgesius and Wilfred Steenbruggen, `The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust` [2019] 19(2) Theoretical Inquiries in Law 291-322

2.2 The Convention as a "Living Instrument"

It is not wrong to say that technology has constituted another world and created another dimension for human lives. The Internet, smartphones, debit cards, social media, and similar technologies not only ease individuals' life but also completely changed their priorities. Paying a bill, travelling somewhere, communicating with someone, or sharing thoughts has never been such easy in the past. For instance, access to the Internet is considered a fundamental right in today's world.[26] Undoubtedly, one of the most changing fields is communication.

Humankind has always found a way to communicate, albeit in different ways such as drawing pictures on the walls, smoke signals, and messages arriving in less than a second. In the past, communication with one who is in other places was harder, cumbersome, and slower. However, in today's world, individuals can talk whenever and in any way they want to communicate such as voice calls, or video calls for no cost via IM applications such as WhatsApp.[27] Since billions of people use IM applications to communicate, those platforms can be regarded as one of the most important communication methods nowadays. Therefore, it should be examined whether communication in IM applications is protected.

Until the 1950s, the focus of the privacy was on physical intrusion on the person. To this date, the ECtHR did not consider that the privacy of information must be protected under Article 8 so that data protection was not in consideration. Information aspects of privacy and the use of databases became a greater concern in terms of their use of banks, governments, and industries in the 1960s. The Court changed its view on the later judgements and ruled that informational aspects of the privacy must also be protected under Article 8, which was a very significant evolution.[28] The ECtHR puts its focus on the Convention as a living instrument, therefore, the implementation of the Convention is being changed following technology and other conditions.[29] This is a very significant improvement as the law cannot easily adapt to the changes coming via innovations and technological developments. The ECtHR adopted a broader interpretation of the relationship between private life and personal information and properly interpreted the article under the "present-day conditions". Thus, information privacy is now considered under the protection of Article 8.

---

[26] Colin Crawford, 'Cyberplace: Defining a Right to Internet Access Through Public Accommodation Law' [2004] 76(2) Temple Law Review 225-276
[27] WhatsApp, 'Making WhatsApp free and more useful' (WhatsApp Blog, 18 January) <https://blog.whatsapp.com/making-whats-app-free-and-more-useful> accessed 02 July 2020
[28] Tyrer v The United Kingdom App no 5856/72 (ECHR, 1978)
[29] Ibid

While regulating the Convention, inherently new technologies could not be predicted. The ECtHR envisaged the "living instrument" approach for the interpretation of the term "correspondence" so that the meaning of "correspondence" has expanded. In line with this, while technology is developing, the Court has started to interpret this term broadly and also included innovations such as mailing in the scope of the protection of this right.[30] It properly ruled that IM applications should be determined under that term in 2017.[31] These decisions of the court ensured that the communication between people was protected regardless of the technology used.[32] With these developments, communication via IM application is considered under the protection of Article 8.

3. Why and How to Provide Confidential Communication

In the next part, why and how communication via IM applications should be confidential will be discussed. First, the importance of enabling privacy and security within communications will be stressed by mentioning the value of data. Second, the method of end-to-end encryption will be analysed.

3.1 Importance of Providing Privacy and Security

In IM applications, communication can proceed with the combination of a large amount of data. Once a person sends a message to their friend, several different types of data are created. The information of the sender, the receiver, time, location, and content of the message could be given as examples to those data. The value of data has sharply grown since its capability to reveal information about individuals. Due to its importance, data is described as the new oil.[33] Indeed, it is better than that because data is never-ending, copiable, can be reshared and reused. Thanks to today's global architecture, there is no longer a barrier in terms of data collecting and sharing. Data capture and analysis systems are incredibly improved. Data of individuals are constantly created or collected once they use a device or a particular service, then, those data are analysed for numerous purposes. Therefore, enabling the security of communication data is a highly crucial responsibility for the IM application providers.

Security and confidentiality of communication are important due to several reasons. For instance, if a provider such as WhatsApp uses individuals' data for other purposes than communication

---

[30] ECHR, 'Background paper for the Judicial Seminar 2020: The Convention as a Living Instrument at 70' (*ECHR*, 2020) <https://www.echr.coe.int/Documents/Seminar_background_paper_2020_ENG.pdf> accessed 12 August 2020

[31] Bărbulescu v Romania App no 61498/08 (ECHR, 2017)

[32] Borgesius and Steenbruggen (n 25)

[33] The Economist, 'The world's most valuable resource is no longer oil, but data' (The Economist's website, 6 May 2017)

or does not provide effective security, there would be serious problems for the users. A huge amount of data is being collected nowadays from individuals' communications because of the convergence of technology.[34] Not only technology is developing but also the way that it is used is developing. In the past, there were analogue phones that could be used only for a limited purpose. However, nowadays smartphones are devices at which nearly every type of communication method is used. That being said, smartphones may host any kind of information. For instance, they can recognise individuals' faces and using people's location information. Whilst an enormous amount of information is collected from different sources, these could be linked with other methods such as machine learning.[35] Along these lines, critical information might be created from unrelated data even though data is not given by individuals. This method can result in the exposure of highly sensitive data; thus, political views or medical conditions of people can be revealed to others. Therefore, the resulting information can be used in many areas, which may be risky for the data subjects. Accordingly, fundamental rights and freedoms are also affected by this evolution. For instance, communication without confidentiality can cause a chilling effect on people's freedom of expression which means that people refrain from invoking their freedom of expression for certain reasons such as the fear of arrest.[36] The chilling effect will be discussed below in detail. Since technology brings new problems and concerns, providers need to have high-security methods and principles to adapt to the new environment.

Innovations can be used for illegal purposes together with its benefits. Communication data are also under a huge threat because of malicious people trying to hack internet users' data. For example, one of both citizens of the United Kingdom is subjected to online crime.[37] In accordance with this research, together with the rate of committing cybercrime, the impact of these crimes has also dramatically increased in the innovation age. Therefore, it is highly significant to provide communication with great security and confidentiality. Also, certain factors make this situation more difficult. For instance, the identities of online crime perpetrators might not be readily found. Hackers attempt to find a bug or any vulnerability while trying to steal or access to information. This constitutes a huge threat for communication between individuals using IM applications such as WhatsApp which has nearly 2 billion users.[38]

---

[34] Stephen B Wicker, Cellular Convergence and the Death of Privacy (1st edn, Oxford University Press 2013) 55
[35] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, And The Future of Law Enforcement (1st edn, New York University Press 2017)
[36] Jon Penney, 'Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study' [2017] 6(2) Internet Policy Review 1-39
[37] The Economist, 'Thieves in the night' (The Economist's website, 17 December 2014)
[38] Jeff Horwitz, 'As WhatsApp Tops 2 Billion Users, Its Boss Vows to Defend Encryption' (The Wall Street Journal, 12 February 2020)

According to Keller, there were various key drivers for confidential communication.[39] Privacy was a secondary driver; however, business confidentiality historically has been the biggest driver of legal requirements for communications, secrecy, and protection. It was for businesses taking advantage of all these new communications, demanding secrecy of those and protection for the communication services.[40] Confidential communication is highly crucial for hindering sensitive information for businesses such as financial statements and information of their clients. From a customer perspective, in a privacy gap occurring in a financial institution, customers may lose their trust in that organization and even the sector.[41] Moreover, this protection is also important for a company's trade secrets. Businesses can only effectively compete with their competitors thereby enabling the confidentiality of their trade secrets.[42] Once such information is mentioned in a conversation on an IM application, both reputation of the company and its ability to compete might be damaged without effective protection.

Not only private companies are using data technologies, but also states utilize these technics in their surveillance activities for certain purposes. Governments have more opportunities to scrutinise people more readily than they had in the very recent past. With the innovation of the Internet, surveillance cost has dramatically declined.[43] The changes in the surveillance abilities of the states can be better understood with the comparison between the terms of "monitorable" and "searchable".[44] As technology develops, the difference between these two has been narrowing. For instance, while a citizen is committing a crime, others could monitor them. However, this moment could not be searched due to the absence of sufficient technology such as CCTV cameras. Similarly, the house of an individual could be searched, nonetheless, it could not be monitored adequately. In today's world, everything is both searchable and monitorable, therefore, more transparent compared to the past.[45]

Beyond increasing the surveillance power of states, this is an area in which there are high justifications for the access and collection of a huge amount of extremely personal data. It is a highly controversial issue in which situations and how the state can use these powers. It is certain that technology provides people with a safer environment and makes the police and competent authorities stronger. Nonetheless, the use of these forces by the states may constitute a violation of people's

---

[39] Keller (n 13)
[40] Keller (n 13)
[41] Peter Swire, 'Efficient Confidentiality for Privacy, Security, and Confidential Business Information' [2003] Brookings-Wharton Papers on Financial Services 273-310
[42] Michael A Epstein and Stuart D Levi, 'Protecting Trade Secret Information: A Plan For Proactive Strategy' [1988] 43(3) The Business Lawyer 887-91
[43] Lessig (n 11)
[44] Lessig (n 11)
[45] Lessig (n 11)

fundamental rights and freedoms such as privacy and the right to communications confidentiality. The problem in question is not whether authorities could scrutinize individuals in today's world, as it is considered inevitable. The question is what the appropriate measures will be and how they should be implemented. These discussions, which have not attracted much attention of the society until today, have been on the agenda of the world with Edward Snowden revelations in 2013.[46] Snowden realised thousands of documents about how the National Security Agency ("NSA") and other intelligence agencies around the world collect data. It is understood that states use highly strong powers to monitor their citizens. This situation can be explained better with an example. The right to privacy and the right to communication confidentiality are rights which states see themselves as parents who left alone their babies, namely, citizens in the cradle, but are still listening to them carefully.[47] However, neither citizens are babies nor states are parents, and the powers of states must be restricted with individuals' fundamental rights and freedoms. In sum, communication made via IM applications must be secure and confidential.

3.2 How to Enable Privacy in The Face of Innovations

Confidential communication is one of the most important elements of human life. For efficient communication, platforms are needed where people can talk one-to-one and have their private conversations without being watched by others. Otherwise, individuals cannot comfortably express their views and feelings. For instance, in a world where people are afraid of being arrested because of their political views, they cannot be expected to freely share their political opinions. Accordingly, users must also trust IM applications to communicate with other people by feeling safe. If not, they may tend not to use these apps and this tendency poses a threat to freedom of thought and freedom of assembly in addition to privacy and freedom of speech.[48] The right to communication confidentiality prevents individuals' conversation, ideas, and feelings to be accessed by undesirable persons.[49] In the past, a letter could be hidden somewhere by its owner. It would be nearly impossible to get information about the letter since it was merely one. However, if that kind of document or a message is in an electronic device such as mobile phones or computers, it can be readily duplicated, accessed, and manipulated without any authorization regardless of whether an encryption method is used.

To handle the hardships discussed, a secure and effective remedy is required. At this point, IM application providers have rushed to help and developed an end-to-end encryption system for their

[46] Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' (The Guardian, 6 June 2013)
[47] Lessig (n 11)
[48] Borgesius and Steenbruggen (n 25)
[49] Borgesius and Steenbruggen (n 25)

applications. E2EE technics are used by IM applications to ensure the privacy of its users.[50] Videos, phone recordings, locations, messages, namely, any information sent via WhatsApp cannot be read by any party, even by WhatsApp, except the sender and the receiver.[51] This is achieved by automatically encrypting each message sent via WhatsApp.[52] With this technique, once the message is sent, it is encrypted with a special key and that can only be decrypted with the key of the receiver via the Signal Protocol.[53] Since no one holds the key including application providers, malicious people such as hackers could not access the code and access the data. By this means, even if somehow a key was decrypted by an unauthorized person, a new key is produced for every new message. Such an encryption method is also useful for the communication of businesses to protect their confidential information. With E2EE IM Applications, they can secure their private information even from the application provider while communicating. Finally, conversations will be safer against state surveillance and may prevent chilling effects on fundamental freedoms. Users do not have to delete messages instantly, and they might keep them on their electronic devices. To provide secure communication, unlawful access to messages that users want to keep should be prevented. According to the ECtHR, Article 8 ECHR applies not only to the time of communication but also after the communication ends.[54] Thanks to the E2EE technology, even if keys that are used for encryption are hacked or revealed, messages that are already transmitted cannot be seen.[55] Using these encryption methods can enable adequate protection for messages also in the post-transmission phase.

However, this E2EE method is only for the content data and it does not protect communication metadata.[56] Therefore, as a large quality and quantity of information can be still revealed from communication metadata, merely access to metadata raises a huge concern. These privacy problems due to access to metadata will be examined below. In terms of the content of a communication, end-to-end encryption is a great solution to enable privacy and confidentiality of communications via IM applications.

[50] WhatsApp (n 1)
[51] Stefan Schuster and others, 'Mass surveillance and technological policy options: Improving security of private communications' [2017] 50 Computer Standards & Interfaces 76-82
[52] WhatsApp (n 1)
[53] WhatsApp (n 1)
[54] Bernh Larsen Holding AS and others v Norway App no 24117/08 (ECHR, 2013).
[55] WhatsApp (n 1)
[56] WhatsApp (n 1)

4. Law Enforcement Authorities vs E2EE Instant Messaging Applications

The next part will discuss whether and what kind of communication data from E2EE IM applications should be used by law enforcement authorities for the prevention of crime and providing national security. Initially, the concept of "going dark" will be examined. Then, three different views on the problems between law enforcement authorities and E2EE IM applications will be analysed. After the discussion of whether authorities should be able to access communication content data of those applications, surveillance on communication metadata will be described.

4.1 The Issue of "Going Dark"

Encryption provides an effective solution for confidential communication so that it is highly significant for human dignity.[57] Nonetheless, it may raise huge concerns in terms of the prevention of crimes. Since no one except the sender and the receiver can see the content, authorities cannot collect content information as digital evidence for investigations.[58] Even though law enforcement authorities request a warrant from the court, that warrant would be useless as accessing the content of the communication that is made via the E2EE IM applications is impossible.[59] Thus, E2EE is a crucial problem for law enforcement authorities to gather evidence, which is defined as "Going Dark".[60] According to the supporters of this concept, malicious persons use E2EE applications to escape from law enforcement authorities.[61] To prevent this and make law enforcement effective, governments and agencies claim that E2EE IM applications should provide authorities with a back door for agencies to access to the content of the communication. [62] Both "Going Dark" and "Back Door" issues will be discussed in the following sections.

4.2 Enabling Security and Prevention of Crimes

Providing law enforcement authorities with effective tools is highly significant in their fight with terrorism and serious crimes. However, in the digital age, this is an extremely hard task for authorities due to the difficulties of pursuing and gathering evidence. Terrorist organisations nowadays use the E2EE application to communicate with each other.[63] They even plan their attacks on those

---

[57] Digital Europe, 'Encryption: finding the balance between privacy, security and lawful data access' (Digital Europe, 16 March 2020) <https://www.digitaleurope.org/resources/encryption-finding-the-balance-between-privacy-security-and-lawful-data-access/> accessed 15 August 2020
[58] Jim Baker, 'Rethinking Encryption' (Lawfare, 22 October 2019) <https://www.lawfareblog.com/rethinking-encryption> accessed 18 August 2020
[59] Charles Duan and others, 'Policy approaches to the encryption debate' (RStreet, 5 March 2018)
[60] Federal Bureau of Investigation (n 3)
[61] Charles and others (n 59)
[62] Andrew Sparrow, 'WhatsApp must be accessible to authorities, says Amber Rudd' (The Guardian, 2017)
[63] Robert Graham, 'How Terrorists Use Encryption' [2016] 9(6) CTC Sentiel

kinds of platforms.[64] Because communication is confidential and highly secured on E2EE IM applications, authorities can't access those content data. However, due to the authorities' mission of providing citizens' security in accordance with the right to life (Article 2) and the right to liberty and security (Article 5) that are regulated by the ECHR, they request E2EE IM application providers to enable a back door.[65] "Back door" can be defined as a hidden bug in an application or a software place by its developer for certain purposes such as allowing authorities to access encrypted communication.[66] Several rights and freedoms that are not absolute can interfere with the requirements that are stated by the Convention. Nonetheless, a back door might constitute a violation of the right to communication confidentiality. For this reason, the balancing issue is highly critic and must be examined very clearly. Otherwise, it may cause serious violations of individuals' fundamental rights and freedoms.

As confidential communication is an important fundamental right, in case of an intervention to this right, different interests must be properly balanced. It can be argued that privacy law has two main concerns: Under what circumstances personal data may be gathered by the governments and how to ensure that they do not cross the limits in this regard.[67] As the ECHR Article 8 states, there must be no interference with the right to respect for private and family life, home, and correspondence so that authorities cannot interfere with individuals' right to communication confidentiality. However, this right is not an absolute right, namely, it has limits and it must be balanced with other fundamental rights, freedoms, and values of society. According to Article 8 ECHR, such interference should be in accordance with the law, necessary in a democratic society, and should pursue a legitimate aim. So that law enforcement authorities are not completely free when they are monitoring individuals and they cannot scrutinize all kinds of information.

4.3 Content Data or Metadata?

This section will discuss which type of data which law enforcement authorities should be able to monitor on IM applications. To examine, the interpretation of the necessity of the ECtHR will be used. In order of interference to be justified, it should be considered necessary in a democratic society.[68] For this reason, separate interests must be reasonably balanced, such intervention must be in

[64] Dipesh Gadher, 'London Bridge terror attack planned on WhatsApp' (The Times, 2019)
[65] Graham (n 62)
[66] Article 29 Working Party, 'Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU' (Brussels, 11 April 2018)
[67] Reed, C., 2004. Internet Law. 2nd ed. Cambridge University Press, pp.1-2,128.
[68] ECHR art 8

accordance with the law and proportionate to the legitimate aims that authorities must pursue.[69] Interception must include sufficient and relevant justifications and must be proportionate to the purpose of the surveillance.[70] Thus, what type of data law enforcement authorities can monitor and to what extent they can scrutinize must be determined according to those requirements.

IM applications process communication data such as the information of the sender and the receiver to enable communication. As a result, it became possible for states to collect and access important information, which can be used to build behaviour patterns, through indirect tools. For instance, the hierarchical structure of a terrorist organization can be understood by combining information between whom communication is made and communication frequency. Indeed, for this reason, governments can force third parties to retain people's communication data for longer than expected. In that way, it can be argued that communication providers may be considered as a state agent holding citizens' data. However, even though processing communication data by communication providers can be justified, access to that information must be subject to strict rules and conditions. It should be stated that the collection of data can be justified for several reasons, as long as access to them is strictly controlled.

E2EE applications make it easier for culprits to commit crimes. Similarly, those applications provide terrorists and criminals with a secure platform to organize their plans which can be highly detrimental to the public. For instance, a criminal in a case had claimed that E2EE is a present from God.[71] In line with this, research demonstrated that one of both individuals living in the UK is a victim of online crimes.[72] The possibility of criminals to connect to the internet with a secret identity and remotely might raise the amount of crime committed in online platforms. Such platforms not only create new environments to commit existing crimes but also enable new sorts of crimes to be committed such as hacking.[73] For example, criminals might benefit from E2EE IM applications to organize terrorist actions or coup attempts.[74] The state must protect the citizens from the occurrence

[69] ECHR, 'Factsheet on Mass Surveillance' (September 2019) <https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf> accessed 10 June 2020
[70] Kokott and Sobotta (n 15)
[71] Senate committee on the judiciary, 'Going Dark: Encryption, Technology, And the Balance Between Public Safety and Privacy' [2015] One Hundred Fourteenth Congress, First Session
[72] John Naughton, 'The evolution of the Internet: from military experiment to General Purpose Technology' [2016] 1(1) Journal of Cyber Policy 5-28
[73] Joss Wright, 'Necessary and inherent limits to internet surveillance' [2013] 2(3). Internet Policy Review, <https://policyreview.info/articles/analysis/necessary-and-inherent-limits-internetsurveillance> accessed 13 March 2020
[74] Yasir Gokce, 'The Bylock fallacy: An In-depth Analysis of the Bylock Investigations in Turkey' [2018] 26 Digital Investigation 81-91

of such crimes and this duty requires the state to have some powers.[75] For this reason, one may argue that governments should be able to access the communication content. Nonetheless, these are extremely risky in terms of fundamental rights and freedoms of individuals, thus, there should be a strong balancing activity.

In terms of the relationship between law enforcement authorities and E2EE IM applications, there are several different views. According to most governments and agencies, due to the situation of Going Dark, law enforcement authorities are inefficient to prevent crimes and proceed with investigations.[76] Some people suggest that E2EE applications must be prohibited.[77] Others argue that E2EE applications must provide a back door for governments to access the communication content.[78] However, privacy supporters believe that providing a back door will raise many concerns and because of technological improvements such as data analysing, authorities have already a large number of powerful methods for surveillance.[79] Even though they cannot access content data of E2EE IM applications as they could with other communication methods in the past, they can enjoy a wide scope of metadata such as call history or location data.[80]

One may claim that the prohibition of E2EE applications is both infringing, disproportionate, and useless for the aim. Similarly, opponents argue that the prohibition of the E2EE applications is not a solution since criminals may readily create a new application depends on the E2EE.[81] Even though a new application can be created easily, the determination and pursuance of those would be easier; as police would know that only users of that application are criminals. For instance, members of a terrorist organization were using "ByLock" to communicate in Turkey and after this fact is revealed, people using "ByLock" were arrested.[82] Nonetheless, in line with the views of opponents, members of the

---

[75] Jarvie, 'Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1' [2003] 9(3) Computer and Telecommunications Law Review 76-81

[76] Federal bureau of investigation, 'Lawful Access' (Federal Bureau Of Investigation's website) <https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch/lawful-access> accessed 01.06.2020

[77] Riana Pfefferkorn, 'The earn it act: How to ban end-to-end encryption without actually banning it' (The Center for Internet and Society at Stanford Law School, 30 January) <http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it> accessed 30 August 2020

[78] Vience Mutiara Rumata and Ashwin Sasongko Sastrosubroto, 'The Indonesian Law Enforcement Challenges over Encrypted Global Social Networking Platforms' [2018] International Conference on Computer, Control, Informatics and its Applications (IC3INA), Tangerang, Indonesia, 2018, pp. 199-203

[79] Riana Pfefferkorn, 'Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?' [2017] 49(5) Connecticut Law Review 1393-1452

[80] Peter Swire, 'The Golden Age of Surveillance' (Slate, 15 July 2015) <https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html> accessed 21 August 2020

[81] Robert E Endeley, 'End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger' [2018] 9(1) Journal of Information Security 95-99

[82] Ismet Karakas and others, 'Turkey: 18 FETO terror group suspects held' (Anadolu Agency, 21 July 2020)

terrorist organization ISIS have used PlayStation 4 to communicate.[83] That being said, even though a particular E2EE application is prohibited, criminals can use other applications to communicate even those for children to play. For instance, once a country prohibited E2EE applications, criminals might easily use the same kinds of applications in another country due to the borderless nature of the Internet.[84] Thus, the prohibition of the E2EE applications would be a useless solution since it does not help the purpose of the prevention of crimes to be succeeded. Moreover, it is a disproportionate remedy since the aim can be satisfied with less intrusive methods as will be discussed in detail in the following parts.

Most law enforcement authorities lobby legislators to regulate a requirement for E2EE applications to provide a back door for them to reveal communication content data. At this point, Article 2 ECHR which regulating the right to life must also be examined. According to provision: "*Everyone's right to life shall be protected by law.*" Depending on this clause, one may argue that law enforcement authorities must access to communication content data to protect citizens. In line with this, a terrorist in the Westminster Attack had got online on WhatsApp a few minutes before the attack.[85] If the UK government was allowed to intercept the WhatsApp account of the terrorist once they suspected, the attack would have been prevented. They could have applied for a warrant from the court and sent it to WhatsApp. Then, WhatsApp could have removed the E2EE merely for that suspected person. It is attractive for criminals or terrorists to choose to plan their activities on those kinds of E2EE platforms. However, merely the existence of a legitimate reason in itself does not justify such interference, and restrictions regarding the protection of personal data must also apply.[86] In that regard, the comparison must be made between harms where police could not access to content data and harms relating to privacy or communication confidentiality where police could access to content data.

It may be argued that when police could not access to communication content data, it cannot collect strong and clear evidence with other methods as they could via content data. It is clear that content data is highly effective and once accessed, there might be no need for any other method to analyse relevant data because everything is clear. According to some governments, not being able to access the content of the communication on E2EE applications creates a safe zone for terrorists so that

[83] Paul Tassi, 'How ISIS Terrorists May Have Used PlayStation 4 To Discuss and Plan Attacks [Updated]' (Forbes, 14 November 2015)
[84] Senate committee on the judiciary (n 71)
[85] Sparrow (n 62)
[86] Digital Rights Ireland Ltd [2014] Court of Justice of the EU Joined Cases C-293/12 and C-594/12, Curia

they should have powers to access the content.[87] For instance, according to the former Director of the FBI, ISIS has been directing its member to E2EE applications to avoid the FBI.[88] However, there are still other methods such as communication metadata that are highly useful to reveal evidence for crimes or terrorist attacks.[89] Thus, where there is a less intrusive method which is also useful for the authorities, that should be chosen even though there might be left more jobs to do on the authorities. Moreover, for some serious crimes, access to communication content data may be the only way to combat it. For instance, malicious persons can use E2EE platforms to share horrific videos relating to child pornography. WhatsApp claims that they have improved a system scanning photos and videos even if they are encrypted and if it founds sexual abuse, bans the content.[90] However, it is still a huge concern because of the dilemma between privacy and children's interest. However, considering the other side of the coin, harms relating to individuals' privacy and their right to communication confidentiality, one may state that the latter damage is more dominant than the former. Where governments have access to content data, this will cause several threats for the individuals' fundamental rights and freedoms as will be discussed below: vulnerability of IM applications and people's information in the face of hacking activities and data technologies, chilling effect on individuals' freedom of expression, will harm business confidentiality and besides, there are still sufficient methods to collect digital evidence which are less intrusive.

Providing a back door contradicts with the nature of the E2EE method as E2EE applications try to create secure communication. These methods achieve a high level of safety since nobody has or can access the relevant key, even the service provider. However, providing a back door means that third parties will have an opportunity to break this encryption. Even if merely one person or entity has the code, another person always can reveal the key.[91] Namely, enabling governments to access those messages will render the E2EE method useless.[92] Once a back door is provided, the application will become vulnerable to malicious persons such as hackers, for example. For instance, if a master key is produced for a government to access merely one mobile phone, many keys can be produced and all mobile phones might be under a huge threat of stealing their data.[93] As hackers may benefit a back

[87] Watt and others (n 4)
[88] Comey James, 'Encryption, Public Safety, and "Going Dark"' (Lawfare, 6 July) <https://www.lawfareblog.com/encryption-public-safety-and-going-dark> accessed 02 August 2020
[89] Rastogi (n 5)
[90] Katie Benner and Mike Isaac, 'Child-Welfare Activists Attack Facebook Over Encryption Plans' (The New York Times, 5 February 2020)
[91] Article 29 Working Party (n 66)
[92] Endeley (n 81)
[93] Tim Cook, 'A Message to Our Customers' (Apple, 16 February 2016) <https://www.apple.com/customer-letter/> accessed 09 August 2020

door that is provided by governments within E2EE IM applications, there is always a possibility that thousands of data are captured by malevolent persons. When considering this with the current technologies such as big data, it can be understood that this poses a threat in terms of several fundamental rights of individuals.[94] Data can be combined with other technics like machine learning which is a type of artificial intelligence-driven form of data analysis. Even though data mining has been happening since the 1960s, certain differences make database hack more dangerous in today's world. Computers are quicker and more powerful so that it is easier to collect much more data. Different kinds of data can be associated readily than in the past. Moreover, individuals are generating much more data nowadays. Since more big data means much data mining, hacking data may harm individuals' rights and freedoms. For example, information about where a person lives may not be considered sensitive data. However, malicious people can put different data in together just as connecting separate dots by having a huge amount of data. They can reveal other information about a person that may not have been provided by them. Considering IM applications offering numerous services from video calls to make payments, enabling a back door means that agencies can observe the individuals' all life. Besides, like machine learning, it is all in the term, is learning from the data, so from itself. Its results may not always be correct. If communication content data from E2EE IM applications is combined with other data with the help of machine learning, even the way of thinking of users can be revealed.[95] Hence, even though states do not misuse a back door, it might cause highly significant damages for individuals due to the malicious people and current technological improvements. In light of those risks, it can be argued that monitoring on content data of E2EE IM applications is not proportionate.

The risks of providing a back door are not only because of the outside factors of the IM applications but also due to the wide range of features of those applications. E2EE IM applications are not just for users to message each other anymore. It can be used for numerous purposes. As an example of WhatsApp, users can communicate with each other either personally or via a group, can make a phone or video call, can share their photos, voice, and video recordings, can share their current locations and even live locations. Once governments are provided with a back door in WhatsApp, for instance, they will be able to scrutinize the users' live location. Moreover, WhatsApp starts a new

[94] Lei Xu and others, 'Information Security in Big Data: Privacy and Data Mining' (IEEE , 09 October 2014) <https://ieeexplore.ieee.org/abstract/document/6919256> accessed 27 July 2020

[95] Carole Cadwalladr and Emma Graham Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (The Guardian, 17 March 2018)

feature enabling its users to make payments via the application.[96] With this novelty, individuals desiring to make transactions without being monitored by the authorities can use WhatsApp's payment system. However, with a back door, this also would be useless for those who want to make a transaction like paying in cash, namely, without being tracked. Thus, numerous novelties on IM applications can be rendered to a dangerous tool to monitor individuals' highly private life once a back door is provided.

The confidentiality of communication is necessary not only for the protection of privacy but also for two additional rationales which are very significant in the information society: freedom of expression and trust in communication services.[97] Communication monitoring may violate freedom of thought and freedom of expression.[98] People should be able to send and receive information without any interference as a nature of the freedom of expression. With a fear of being arrested, individuals cannot freely express their opinions and beliefs. For example, while scrutinizing their messages; ethnicity information can be revealed by law enforcement authorities. That being said, citizens might try to keep themselves in the mainstream views and behaviours to avoid any possible actions of the police. Intrinsically, this affects people's improvements and democratic involvement.[99] Whether a person feels chilling effect depends on the individual. For example, somebody who is in the mainstream in terms of ethnicity, religion, or some political association can feel comfortable while those who are outside of the mainstream tend to be more aware of their behaviours. To prevent such a chilling effect, for a monitoring process to be necessary, different interests must be properly balanced. Sensitive data may be revealed from communication between individuals. This can cause profiling that results in discrimination which may affect individuals' business and personal life. Moreover, as mentioned above, if a back door is provided, there might always be a possibility of information subject to business confidentiality is revealed by both the governments and the third parties. Information such as trade secrets and financial information cannot be safe in this situation so that they may tend to not use E2EE IM applications. Since those applications are highly useful for them to communicate, it may also negatively affect their business. The right to communication confidentiality is the guarantee of freedom of speech and business confidentiality as well as the privacy of people.

---

[96] WhatsApp, 'Bringing Payments to WhatsApp for People and Small Businesses in Brazil' (WhatsApp Blog, 15 June) <https://blog.whatsapp.com/bringing-payments-to-whatsapp-for-people-and-small-businesses-in-brazil> accessed 29 August 2020

[97] Borgesius and Steenbruggen (n 25)

[98] Big Brother Watch and Others v The United Kingdom App nos 58170/13, 62322/14, and 24960/15 (ECHR, 2018)

[99] Daragh Murray and Pete Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' [2019] 52(1) Israel Law Review 31-60

Considering the discussions above, one may conclude that governments' ability to access the communication content data of E2EE IM applications cannot be considered proportionate or necessary in a democratic society. As stated, there are less intrusive methods that authorities are already using. One of the most important methods can be regarded as using metadata since it helps to reveal much information and evidence. There are traditionally very different rules about how content and metadata are handled, which are gradually coming together. Similarly, EU e-privacy regulation is trying to diminish this historic distinction between content data and metadata, and it begins to bring these closer.[100] Accordingly, both types of data could lead to very sensitive information to be revealed. Communication data may be separated into content data and metadata. This classification may be explained with the "letter in an envelope example".[101] An envelope at its outside has information of the receiver, the sender, the addresses of them, and maybe the time that letter has been sent via a stamp. At the same time, the envelope includes a letter inside, which is private and cannot be read without opening the envelope. That being said, there is a clear privacy distinction between the letter and the information on the outside. The letter can be described as "content data", and the information on the outside can be described as "communication metadata". So that content of the letter would be heavily protected, but the communications data at the outside of the envelope would be much less. However, as time goes on, the outside information gets more complicated and starts to disclose much more information about human lives. Indeed, sometimes it reveals far more than what the content is because of the elements such as geolocation and time so that all the patterns of all the texts could be known.[102]

In E2EE applications, content data includes messages, videos, both voice and video calls, photos, location, and so on. Metadata includes information such as the parties of communication, its destination, time, length, type, frequency, used equipment, and the parties' names and telephone numbers.[103] In the case of E2EE IM applications, important information such as contact lists is added to what metadata covers. A surveillance activity might take days or months, and at this time, a huge amount of metadata can be captured by the authorities. So that very detailed behaviour patterns of individuals could be built up. In sum, even though communication content data cannot be considered proportionate and necessary in a democratic society, governments can access metadata by providing the requirements of Article 8 ECHR. For this reason, it can be argued that for surveillance activities

[100] Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in
electronic communications and repealing Directive 2002/58/EC (Regulation
on Privacy and Electronic Communications)' COD (2017/0003)
[101] Keller (n 13)
[102] Rastogi (n 5)
[103] Digital Rights Ireland (n 86)

on E2EE IM applications, law enforcement authorities should not monitor content data. It seems possible for them to scrutinize metadata. However, due to the highly infringing nature of this surveillance, this type of monitoring should be restricted. Surveillance on metadata will be examined in the following section.

5. How to Scrutinize Metadata

As mentioned before, surveillance on communication metadata on E2EE IM applications is an interference with Article 8. To realize whether the intervention can be justified, Article 8(2) should be pursued.[104] Accordingly, the intervention should be in accordance with the law, necessary in a democratic society, and should pursue a legitimate aim. First, this chapter will examine accordance with the law of surveillance on metadata of E2EE IM applications. Then, how monitoring is determined as necessary in a democratic society will be explained. Finally, what should be the legitimate aim of the surveillance will be mentioned.

5.1 In Accordance with The Law

According to the ECtHR, to be in accordance with the law, the surveillance must be covered by domestic law, in accordance with the rule of law, accessible; and the consequences of the surveillance could be foreseen by individuals.[105]

5.1.1 Domestic Law

For interference to be compatible with Article 8, the interference must be regulated by national law.[106] Domestic legislation must not be regulated in a general scope, but in detail.[107] To be clear, legislations regulating general communication surveillance could not satisfy this requirement. For instance, domestic regulations must specifically refer to IM applications to be in accordance with the law rather than generally referring to surveillance on communication data.

The ECtHR states that governments not only take passive measures to protect this right but also it must regulate positive obligations at which states take action to guarantee the privacy of individuals.[108] In the absence of an active attempt to prevent violations of states, there will be a

[104] ECtHR, 'Guide on Article 8 of the Convention – Right to respect for private and family life' (European Court of Human Rights, 30 April 2020) <https://www.echr.coe.int/documents/guide_art_8_eng.pdf> accessed 07 June 2020
[105] Benedik v Slovenia App no 62357/14 (ECHR, 10 September 2014)
[106] Ibid
[107] ECtHR, *Amann v Switzerland* App no 27798/95, ECHR 2000-II, para. 76.
[108] Airey v Ireland App no 6289/73 (ECHR, 1980)

violation of the right to privacy. This also applies to the right to communication confidentiality.[109] States must take appropriate actions for individuals to have secure and effective communications on E2EE IM applications. According to the ECtHR, it is significant to examine whether the implementation of the safeguards is supervised, and domestic regulations enable any remedies and notification instruments.[110] For example, even though there is no specific prohibition for service providers such as WhatsApp who legally store the metadata of users to comply with the requests of the authorities, if the limitations or the extent of the authorities' discretion are not regulated, this surveillance activity will not be in accordance with the law.[111]

The Court has published six minimum requirements for the interception of communication data for criminal investigations, then, it ruled that the same requirements are also applied to the national security purpose.[112] As mentioned, since the Convention has ruled IM applications and metadata are also under the protection of Article 8 with its "living instrument" perspective, the same requirements can be considered valid on surveillance on E2EE IM applications. Accordingly, while determining the intervention of communications metadata, to prevent the misuse of authorities, the following elements must be pursued: the nature of offences causing to the intervention, description of the categories of people whose communications are intervened, time restrictions on the length of the intervention, the process for analysing, using, and keeping the information collected, safeguards concerning sharing the communication data with others and in what situations data should be erased or destructed.[113] The infringing nature of surveillance activities on communication metadata of E2EE IM applications can be decreased with these safeguards.

In addition to the requirement of regulating surveillance in national law, those domestic regulations must be accessible, foreseeable, and clear.[114] Domestic law must demonstrate adequate clarity, enable sufficient security versus misuse of power and wide discretion on the competent authorities to monitor and analyse communications. Namely, the process of choose intervened communication data for its analyse, sharing, storage and destruction must be accessible to individuals.[115] Moreover, where monitoring is foreseeable by individuals, this also helps surveillance to be kept in limitations stated by the regulations.[116] That being said, while individuals use WhatsApp,

[109] Golder v The United Kingdom App no 4451/70 (ECHR, 1975)
[110] Roman Zakharov v Russia App no 47143/06 (ECHR, 2015)
[111] Malone v The United Kingdom App No 8691/79 (ECHR, 1984) para 87
[112] Zakharov (n 110)
[113] Big Brother Watch and Others (n 98)
[114] Silver and Others v the United Kingdom App no 5947/72 (ECHR, 1983)
[115] Liberty and Others v UK App no 58243/00 (ECHR, 2008)
[116] Silver and Others (n 114)

they should know that their communication metadata must be monitored provided with certain safeguards. However, in terms of adjusting foreseeability, a reasonable degree is adequate for individuals as absolute foreseeability is not possible due to the nature of surveillance activities.[117] These requirements enable monitoring to be in the appropriate boundaries.

Whilst technology developing, the same technology can be used for both criminal and policing purposes. The police or law enforcement could justify new technologies to make policing more effective, regardless of what technologies are being used for criminal purposes. A technological improvement that makes individuals more secure can also make law enforcement force more effective. For example, with a certain machine learning technology, communication data that is taken from WhatsApp could be combined with other data, and important information can be revealed. To determine whether a specific technology should be used, it is substantial to assess under what circumstances this technology will be used since there may be an incremental loss of privacy. If circumstances that the technology will be used are clear to individuals, it will also be understandable what the safeguards should be and how they should operate. Using a new technique for surveillance is not in question anymore, the question is about appropriate safeguards. Otherwise, people may tend not to use such E2EE IM applications and cannot effectively invoke their right to communication confidentiality. National regulations must be sufficiently clear so that individuals can understand how much the discretion of states is and how they use their powers.[118] In brief, for interference to the right to communication confidentiality to be justified, a surveillance activity must be prescribed by law in a foreseeable, accessible, and clear way.

5.1.2 Rule of Law

When determining metadata surveillance, it is not sufficient such surveillance is compatible with the national law, it must also be in accordance with the rule of law, namely, "the quality of law".[119] Compatibility with the rule of law principle can be effectively enabled via sufficient safeguards.[120] States have huge powers and predominance over the individuals as agencies can monitor people's communication metadata on IM applications. To protect individuals, sufficient limitations must be implemented over those powers, otherwise, such monitoring would not be in accordance with the rule of law.[121]

---

[117] Slivenko v Latvia App no 48321/99 (ECHR,2003)
[118] Silver and Others (n 114)
[119] Halford v the United Kingdom App no 20605/92 (ECHR, 1997)
[120] Kruglov and Others v Russia App no 11264/04 and 15 (ECHR,2020)
[121] Karabeyoğlu v Turkey App no30083/10 (ECHR, 2016)

In terms of safeguards, one of the most important differences between processing for policing purposes and commercial purposes; the latter is very limited while a wide collection of data is required for the former. Namely, processing data for policing is very permissive especially in the initial collection since there are many legitimate reasons such as national security to collect a huge amount of metadata. How to control the metadata after the initial collection is a much more critical concern in surveillance activities. Data subject rights such as the right to access are limited or postponed in this kind of processing, for instance, they are not be told that they are being investigated. That being said, it can be argued that safeguards for surveillance activities are mainly ex-post since they arise after the event. In accordance with this, what remedies might finally arise once the collection of data is completed is important.

For compatibility with the rule of law, sufficient safeguards should be implemented. For example, collected metadata should be retained for a limited time, otherwise, merely for this reason, surveillance on E2EE IM applications may be considered a violation of the Article 8 ECHR.[122] These measures are significant factors to protect the fundamental rights and freedoms of individuals as violating impacts of surveillance can be diminished in this way. It is important to apply data privacy in present-day living conditions since that is the only way the safeguards are going to work properly. These measures should be implemented practically and effectively rather than in a theoretical and unrealistic way.[123] For example, the prior judicial review authority must be impartial, and not an institution which automatically approves every request. The way of regulating those in national law is highly important. Domestic law must be clear to implement adequate safeguards to protect individuals' rights and freedoms.[124]

According to the Court, safeguards must be implemented in three phases: the initial order of surveillance, during surveillance, and after surveillance. Since the first two steps with their review processes intrinsically proceed without a monitored person's knowledge in monitoring metadata of E2EE IM applications, safeguards must be strictly implemented to protect their rights. Policing is different from other areas and has separate justifications which may help police to avoid those kinds of notices. Generally, crimes or terror attacks happen very quickly so that it may not possible to notify individuals. Without such notification, individuals cannot use their rights against law enforcement authorities such as the right to access. These limitations must not become a rule instead of exceptions

[122] S and Marper v The United Kingdom App no 30562/04 and 30566/04 (ECHR, 2008)
[123] Airey v Ireland (n 108)
[124] Liberty and Others v UK (n 115)

and must be in accordance with the principles of necessity and proportionality.[125] Nonetheless, in today's world, governments must combat threats to their citizens such as terrorism, thus in those circumstances, states must have powers for national security as an exception.[126] The question is that after capturing a huge amount of metadata, how police deal with them. At this point, it is proper to consult an impartial supervisory judgment authority. After the surveillance is done, namely the third step, surveillance subjects must be informed subsequently and retrospectively for efficient remedies and measures versus the abuse of authorities as long as it does not endanger the purpose of the surveillance.[127] Appropriate measures must be implemented not only at a certain stage of the surveillance process but during the entire surveillance. Besides, an automated system can be set up to remind authorities of relevant measures, such as time restrictions.[128]

There are two significant safeguards worth mentioning in terms of surveillance on metadata of IM applications: Time limits for data retention and erasure of data and data subject categories.

5.1.2.1 Time Limits for Metadata Retention and Erasure of Metadata

Proper time limits for metadata retention and erasure of metadata should be set to prevent governments from reusing the metadata that they collected for other purposes. These limits may be implemented to periodically control whether the storage of information is required.[129] They must be objectively determined in accordance with the surveillance and metadata storage purposes, taking into account the effects on different categories of data subjects such as witnesses or victims.[130] Because information on different categories of data subjects serves different purposes in surveillance, applying the same limits to all of them may lead to unfair consequences. Only a failure to regulating time restrictions can be considered a violation of the fundamental rights of individuals.[131] As the Court stated, the blanket and indiscriminate nature of the power of retention are not compatible with Article 8.[132] According to the ECtHR, there is a pressing need to collect a huge amount of data for the prevention of crime. There may be a justification for retaining metadata indefinitely for people, for example, who have been convicted of a serious offense. Nonetheless, at this point, the problem of innocent people arises. Information about an individual who is convicted with a serious crime may

[125] Article 29 Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (WP 258, 29 November 2017)
[126] Klass and Others v Germany App no 5029/71 (ECHR, 1978)
[127] Zakharov (n 110)
[128] Article 29 Working Party (n 125)
[129] Law Enforcement Directive art 5
[130] Article 29 Working Party (n 125)
[131] S And Marper v The UK (n 122)
[132] S And Marper v The UK (n 122)

involve data of other people who are innocents. For example, even though a person is criminals, they might have many innocent people on their WhatsApp contact list. However, storing metadata of innocent people also violates their rights to data protection, moreover, there is no sufficient justification to store highly protected information of those individuals.[133] Even though it is difficult to remove their information from all documents that there is justification to store for a longer time, police are responsible for the database that they created and they must keep it lawful. Similarly, the need for retention must be considered a case-by-case basis. Categories of data must be examined in addition to the age of data subjects.

5.1.2.2 Data Subject Categories

During metadata surveillance, different categories of people should be treated differently. For example, victims or witnesses must be categorically dealt with differently from convicted persons. Once accessed to someone's WhatsApp account, for example, authorities may collect hundreds of people's information, which can be described as incidental capturing.[134] That being said, hugely personal data of innocent people could be collected and stored in this way. Indeed, in some countries, there are crucial studies to create a very comprehensive database of personal data from people who were suspected of a crime at any time for the prevention of crime such as IDENT1.[135] Moreover, law enforcement authorities have started to use big data technology to associate individuals' data with other information that they already have.[136] For instance, while scrutinizing the WhatsApp call history of every people, a comprehensive map of associated people can be created. This raises some privacy concerns, particularly for innocent people.

---

[133] Catt v The United Kingdom App no 43514/15 (ECtHR, 2019)
[134] Elizabeth Goitein, 'Another Bite out of Katz: Foreign Intelligence Surveillance and the "Incidental Overhear" Doctrine' [2018] 55(1) American Criminal Law Review 105-125
[135] UK Home Office, 'Forensic Information Database Service (FINDS): International DNA and Fingerprint Exchange Policy for the United Kingdom' (UK Government, 8 July 2019) <https://www.gov.uk/government/publications/international-dna-and-fingerprint-exchange-policy-for-the-uk/forensic-information-database-service-finds-international-dna-and-fingerprint-exchange-policy-for-the-united-kingdom> accessed 13 July 2020
[136] Wicker (n 34)

5.2 Necessity

An intervention to be justified, it should be necessary in a democratic society.[137] Namely, as mentioned, the interference must have sufficient and relevant justification and must be proportionate.

It is important to determine that if commutation metadata is under Article 8 ECHR. The collection of metadata was first recognized by the ECtHR in 1984.[138] The Court has ruled that "metering" should be considered separately from the interception of communication. Even though the Court subjected violations about metadata to a less stringent test, it ruled that metadata regarding phone calls must be protected.[139] In further cases, the ECtHR has also considered that Article 8 also encompasses metadata concerning internet usage, mail address in 2007, and IM applications in 2017.[140] In conclusion, it can be said that metadata is protected under Article 8 irrespective of which technology is used. However, according to the Court, surveillance on metadata is not as serious violation as surveillance on the content of the communications. Some authors argue that this can be understood as metadata should be processed for an effective service to be provided by the operators.[141] Nonetheless, even though providers can lawfully collect and process metadata, it does not mean that surveillance activities on that metadata are less serious infringement. In the past, authorities inherently had to read outside information of the letter to deliver it even though they were not allowed to read the content. However, it was not possible to reveal sensitive data from metadata as much as now. Nowadays, IM application providers process a large quantity of metadata to run the applications effectively. Metadata gets far more complicated and begins to change individuals' lives more transparent.[142] Sometimes more information can be revealed from metadata than the content data. For instance, very detailed patterns of behaviours can be built from this "outside" information such as who the user is contacting, where, when, and how often they are communicating. The relationship between individuals can be easily understood this way.[143] Metadata can be readily analysed than content data and while processing metadata, governments could get information from numerous individuals as it is not expensive as much as processing content data.[144] Furthermore, the contact lists of the user of an

[137] ECHR art 8
[138] Malone v The UK (n 111)
[139] Ibid
[140] Copland v The United Kingdom App No 62617/00 (ECHR, 2007)
[141] Borgesius and Steenbruggen (n 25)
[142] Rastogi (n 5)
[143] Ibid
[144] Borgesius and Steenbruggen (n 25)

IM application may be revealed via processing metadata, thus, capturing data of other users is extremely easier than communication content information.

There are certain types of surveillances proceeded by states to protect the citizens which bulk retention or interception constitutes one of the most important methods.[145] Bulk surveillance can be defined as the state's capability of access to numerous people's data even though there is no suspicion in terms of national security or serious crime.[146] In the past, there was no concern regarding bulk surveillance as policing had been encompassing only individual notes or tapping phones rather than bulk communication data collection and retention.[147] Nonetheless, in today's world, the communication data of millions of people are scrutinized. This extraordinary change has enabled states to access much data and it caused a new concern of state intelligence powers. If those powers are abused, intrinsically innocent citizens may be affected negatively and, in this possibility, lack of confidence may arise.[148] Thus, the ability of law enforcement authorities to monitor communication metadata must be necessary and proportionate.

To determine whether monitoring is necessary, relevant harms must be examined. First, where law enforcement authorities could not access metadata; it may be extremely difficult to find connections between people or to identify unknown persons in a crime organization. Surveillance on telecommunication networks might not be proper since criminals tend to use E2EE IM applications. Different connections can be revealed with interrogations of suspected persons; however, it might take a long time and might be cumbersome. As a result, law enforcement authorities cannot properly do their job, and crimes or terrorist attacks might not be prevented so that public security may not be provided. Then one may argue that more intrusive methods cannot be taken into account in this discussion because metadata is a strong information revealing tool. Second, where law enforcement authorities could access to metadata; due to the nature of metadata, it might be easier to reveal the behavioural patterns of individuals and the map of a crime organization by examining call history and the frequency of calls. Authorities might have an efficient tool to fight with serious crimes so that they can keep the public safe. At the same time, due to its nature, access and use of the metadata can be

[145] David Anderson, 'A Question of Trust' (UK Government, June 2015) <https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review> accessed 01 August 2020
[146] Daragh Murray and Pete Fussey (n 99)
[147] Keller (n 13)
[148] David Anderson, 'Report of the bulk powers review' (UK Government, 19 August 2016) <https://www.gov.uk/government/publications/investigatory-powers-bill-bulk-powers-review> accessed 01 August 2020

highly intrusive if sufficient safeguards are not provided. For this reason, one can conclude that surveillance on metadata should be restricted, however, it is necessary.

There is an ongoing debate about allowing bulk surveillance. Because to identify the members of a crime organization consisting of unknown people, the only means can be bulk surveillance via capturing all communications and relationships of the known suspected person. This will make revealing the organization since suspected people may contact unknown members. From the examination of the communications data, crime organizations and the hierarchy amongst them can be revealed. Furthermore, where some people use particular software to be anonymous, they can also be found from metadata of individuals. It would be useless for suspected persons to hide their identities with this method. When metadata is compared with the whole data stored until that day, it is highly possible to find identities and patterns.[149] So that bulk metadata retention seems highly useful for the prevention of crime. Nonetheless, such a program must be proportionate thereby specifying appropriate time length and how to keep, manage, and access those data.[150] It must be limited thereby organizing according to whether they are strictly necessary and only if there is a suspicion of serious crime.[151] General and indiscriminate, namely, blanket data retention programs are incompatible with fundamental rights and freedoms.[152]

Another issue with bulk metadata retention is that it may also constitute a violation of freedom of expression and may create a chilling effect on individuals. Importantly, during surveillance, not only the suspected persons are monitored, but also people who there is no proof that they have a connection with any crime, comprehensively. Namely, every people, every telecommunication, and every metadata without any separation and any exception is affected by the monitoring activities.[153] As metadata retention includes every people who are communicated, appearing to be associated with suspicious people can be a fearful situation for others. For example, people may be afraid to communicate with friends who are suspected of a crime because they too may become suspects for that very reason. For this reason, this also may cause a chilling effect on journalists. Since that, surveillance must be restricted to a serious crime and must be reviewed by a prior authority.[154] Besides,

[149] Daragh Murray and Pete Fussey (n 99)
[150] Digital Rights Ireland (n 86)
[151] Daragh Murray and Pete Fussey (n 99)
[152] Tele2 Sverige AB and Tom Watson [2016] Court of Justice of the EU Joined Cases C-203/15 and C-698/15, Curia
[153] Digital Rights Ireland (n 86)
[154] Big Brother Watch and Others (n 98)

six minimum requirements stated by the Court are also important here as the Court referred the same requirements for communication metadata surveillance.[155]

Even if there is a justification for the collection of metadata, there should be different justification for access to those metadata. Furthermore, access must be strictly controlled, otherwise, authorities may readily use the collected metadata for other purposes than the reason for the collection. In continuation, data could be shared and information on who has accessed the metadata may be lost. To prevent those possibilities, surveillance activities must be associated with a described operation and access to collected metadata must be limited with that operation.[156] As stated, information about individuals who are not suspected of a crime can be accessed via others' metadata so that the retention issue is highly critic since there is no legitimate reason for the storage of their metadata. A similar problem was raised with the Directive 2006/24/EC which obliges publicly available telecommunication service providers to store metadata for a time determined by law for purposes such as prevention of crime and national security. Then, the directive was invalidated by the Court of Justice of the European Union ("CJEU") in its landmark case Digital Rights Ireland since it did not determine a proper time for data retention and sufficient safeguards.[157]

5.2.1 How to Collect Communication Metadata

Authorities may gather communication metadata from application providers such as WhatsApp in several ways: They can request metadata from the provider, use spy software and collect the terminal equipment. The first two methods will be examined in the next section.

Service providers may require process communication metadata of individuals to provide them with effective service and to enable the functionality of their service. Similarly, IM applications store information such as the participants, time, frequency, and location of the communication. While the content of the communication is encrypted, it cannot be revealed by anybody. However, information about communication metadata can be seen by the E2EE IM applications providers such as WhatsApp. Users have to accept that their metadata is processed to use the service. Law enforcement authorities or police may desire E2EE IM applications to reveal the communication metadata of their users. As discussed, it is highly contentious whether governments should be able to access metadata since metadata may help authorities to learn a huge amount of information about numerous individuals. Due to the risks of the metadata surveillance of governments, appropriate safeguards must be implemented.

---

[155] Big Brother Watch and Others (n 98)
[156] Daragh Murray and Pete Fussey (n 99)
[157] Digital Rights Ireland (n 86)

Accordingly, the CJEU has ruled highly significant decisions in 2014 where it invalidates the Data Retention Directive of the EU.[158] Importantly, it stated that this surveillance is disproportionate and unprovided with sufficient safeguards. Moreover, such a surveillance activity causes people to perceive that their private lives are under persistent monitoring. In its further judgement, the CJEU stated that service providers should not be forced to keep individuals' metadata under a blanket obligation.[159] Accordingly, the CJEU properly ruled that a large amount of metadata retention is not proportionate surveillance and poses a threat to individuals' privacy and other rights and freedoms even if surveillance is successful to prevent terrorist attacks.[160] Requesting communication metadata form WhatsApp should be subject to prior judicial authorization.[161] Even though this method is not a completely proper way, one might argue that it is reasonable enough provided that authorities must strictly balance different interests.

Another method can be using spyware by governments or law enforcement authorities to monitor individuals' electronic devices such as laptops and mobile phones. Even though this method seems like a science fiction movie for many people, there are countries using spyware nowadays such as The United Arab Emirates and Panama.[162] Thanks to those spyware law enforcement authorities could access the camera, the microphone, or directly the screen of the device.[163] E2EE IM applications can be run via electronic devices such as mobile phones, tablets, and computers. Similar to the traditional privacy view focusing on property rights, the EU e-Privacy Directive mentions that terminal equipment of users must be considered in their private area.[164] Access to information in these devices is a violation of individuals' property rights so that they also must be protected. In this way, authorities could access nearly every data in the equipment, even communication content data of E2EE IM applications. As discussed above, accessing content data of the E2EE IM applications may be determined as a serious violation of fundamental rights and freedoms. In line with this, the purpose of the authorities to apply for this method might be the collection of evidence. Moreover, with this method, even though law enforcement authorities specifically desire to target the content of the communication, capturing and recording data will be much larger as once they access to the equipment, they will be able to collect all data within the particular application or the equipment. With a less

[158] Digital Rights Ireland (n 86)
[159] Tele2 Sverige AB and Tom Watson (n 152)
[160] Ibid
[161] Big Brother Watch and Others (n 98)
[162] Ahmed Azam and David D. Kirkpatrick, 'Hacking a Prince, an Emir and a Journalist to Impress a Client' (The New York Times, 31 August 2018)
[163] Federal bureau of investigation, 'Going Dark' (n 3)
[164] 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 [2002] OJ 2 201/37, recital 24

intrusive method such as accessing metadata, the same purpose can be satisfied. Namely, if the authorities had not got such an option, they would still enjoy individuals' communication data which is information revealing enough. Furthermore, if the authorities use that method, this may cause a chilling effect on freedom of expression and may damage business confidentiality. In the data protection perspective, hacking into a piece of terminal equipment such as mobile phones are considered property interference.[165] During surveillance, individuals' devices that any data flowing through such as mobile phones and laptops are being manipulated so that it is intrusive enough that people's device is used to process data.[166] In other words, regardless of whether the processed data is personal or not, using individuals' property to process data constitutes a sufficient violation. Thus, it can be argued that it is neither necessary nor proportionate. Using spy software constitutes more infringing than requesting access from the provider, and it can be said that this method should not be used for these purposes.

5.3 Legitimate Aim

According to Article 8 ECHR, for interference with Article 8 to be justified, authorities should pursue a legitimate aim. Accordingly, those interests are illustrated as "*in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*" Competent authorities have a wide margin of appreciation in deciding the tools for enabling the legitimate purpose of national security.[167] Nonetheless, this discretion is not exempt from audit but is subject to both regulations and the Court decisions.[168] If there is a possibility that monitoring weakens democratic society, sufficient and efficient measures against abuse must satisfy the ECtHR. Determination of this is a case-by-case analysis including the safeguards' scope, length, nature, grounds for implementing them, authorized agencies to implement and supervise, and remedies stated by domestic law. [169] As mentioned, criminals tend to use E2EE IM applications to escape from enforcement authorities. Because metadata is highly useful for the prevention of crime and national security, these seem proper legitimate aims for communication metadata surveillance on E2EE IM applications. However, all those processes must be sufficient to ensure that the intervention is necessary in a democratic society to satisfy the legitimate aim.[170] As mentioned above, one can

[165] David Anderson (n 148)
[166] Council of the European Union (n 100)
[167] Klass and Others (n 126)
[168] Kvasnica v Slovakia App no 72094/01 (ECHR, 2009)
[169] Zakharov (n 110)
[170] Barfod v Denmark App no 11508/85 (ECHR, 1989)

conclude that the only way to effectively fight with serious crimes is access and usage of communication metadata in terms of E2EE IM applications provided that powerful and sufficient safeguards are applied.

The requirement of legitimate aim raises huge concerns in surveillance activities. As surveillance operations aim to ensure public security, prevention of crime and national security could be accepted as an appropriate aim.[171] Nonetheless, broad terms such as national security should not be considered a proper legitimate aim and governments must specify it.[172] This also may help to more clearly determine the scope of surveillance, thus, surveillance activity can be considered in accordance with the law. The term "national security" is highly contentious, particularly when defining its boundaries. For example, while the LED is implemented to regulate the processing of personal data for crime-related purposes, it does not apply for national security issues.[173] Even though this term is not clearly defined by the European Union Law or the CJEU, it can be generally said that the operations of intelligence and security agencies are considered under this term.[174] It can be argued that the lack of a precise definition of the concept of national security makes it difficult to draw the limits of the legitimate aim. However, this hardship can be satisfied with effective measures such as prior judicial authorization.

6. Conclusion

The aim of this dissertation is answering the question of whether law enforcement authorities should be provided with a back door on E2EE IM applications to monitor communication content data, then, how to perform appropriate surveillance on E2EE IM applications.

It should be stated that confidential communication is highly significant due to several reasons such as freedom of expression, business confidentiality, and privacy. For this reason, the right to communication confidentiality is regulated as a separate right under Article 8 ECHR. Within the "living instrument" approach of the ECtHR, the ECHR is interpreted according to present-day conditions. Thus, users of IM applications enjoy the protection of the right to communication confidentiality.

Within the recent developments, the value of data has sharply increased. Technologies such as machine learning and hacking have become a huge threat to individuals' privacy as they can reveal

---

[171] Digital Rights Ireland (n 86)
[172] David Bainbridge, Introduction to Information Technology Law (6th edn, Pearson Longman 2008) 636
[173] Law Enforcement Directive, recital 14
[174] Article 29 Working Party, 'Working Document on surveillance of electronic communications for intelligence and national security purposes' (WP 228, 5 December 2014)

people's sensitive information. For these reasons, tools enabling IM applications with security and privacy protection is crucial. To succeed in these aims, IM applications began to use the end-to-end encryption method. This raises national security concerns for law enforcement authorities since it hinders them to monitor communication content data. However, from a privacy perspective, authorities' access to communication content data on E2EE IM applications is extremely problematic and they have already sufficient methods to fight with crimes.

Several solutions are suggested for this dilemma. Some suggest that E2EE IM applications must be prohibited as they provide criminals with a safe zone to commit crimes, whilst some claim that a back door should be provided for the authorities to access content data. Nonetheless, providing a back door for the authorities is highly dangerous for many reasons. Once a back door is created in an application, this means that there is a bug in an application, and it is vulnerable to malicious attacks. So that people's information is under a huge threat. Furthermore, a possibility that communication content can be accessed by the authorities may cause a chilling effect on individuals and this might push them not to express themselves freely. Moreover, business confidentiality may also be damaged in case of a back door.

Where police could not access communication content data of E2EE IM applications, it may be harder to find evidence for serious crimes. Then, due to their nature, some crimes might only be prevented with access to content data. However, the other side of the coin has dominance and there is still a method for prevention of crime and national security: Surveillance on metadata. Since that, one may claim that surveillance on content data of E2EE IM applications should not be allowed, thus, a back door must not be created.

With monitoring metadata, highly sensitive information can be revealed, and strong evidence and relationship between individuals can be revealed. It can be argued that surveillance of content data and metadata is nearly identical. For this reason, even though there may be justifications for surveillance on metadata of E2EE IM applications, it must be restricted within the necessities of a democratic society and the principle of proportionality.

In line with Article 8, surveillance on metadata must be in accordance with the law. So, communication metadata on IM applications must be regulated with domestic law, accessible, foreseeable, and compatible with the rule of law. At this point, it is important to provide appropriate safeguards such as time length for data retention and separate rules for different data subject categories. Then, communication metadata surveillance on E2EE IM applications must be necessary in a democratic society. Public interest and individuals' interest in privacy and communication

confidentiality should be strictly balanced. States must be kept in the lawful boundaries and surveillance must be proportionate. Finally, monitoring might be compatible with the legitimate aims of national security and the prevention of crimes. However, surveillance must not exceed what is necessary for the legitimate aim and it should be still considered whether that surveillance activities have sufficient and relevant justifications.

For these reasons, it can be stated that a back door for authorities to monitor content data should not be provided. Even though surveillance on communication metadata of E2EE IM applications can be justified, monitoring should be in appropriate limits.

Reference List

Primary Resources

EU legislation and cases

Digital Rights Ireland Ltd [2014] Court of Justice of the EU Joined Cases C-293/12 and C-594/12, Curia

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 [2002] OJ 2 201/37

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ 2 281/31

ECtHR, *Amann v Switzerland* App no 27798/95, ECHR 2000-II, para. 76

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 119/1

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ 2 119/89

Tele2 Sverige AB and Tom Watson [2016] Court of Justice of the EU Joined Cases C-203/15 and C-698/15, Curia

European Court of Human Rights

Airey v Ireland App no 6289/73 (ECHR, 1980)

Barfod v Denmark App no 11508/85 (ECHR, 1989)

Bărbulescu v Romania App no 61498/08 (ECHR, 2017)

Benedik v Slovenia App no 62357/14 (ECHR, 10 September 2014)

Bernh Larsen Holding AS and others v Norway App no 24117/08 (ECHR, 2013).

Big Brother Watch and Others v The United Kingdom App no 58170/13, 62322/14, and 24960/15 (ECHR, 2018)

Catt v The United Kingdom App no 43514/15 (ECtHR, 2019)

Copland v The United Kingdom App No 62617/00 (ECHR, 2007)

Golder v The United Kingdom App no 4451/70 (ECHR, 1975)

Halford v the United Kingdom App no 20605/92 (ECHR, 1997)

Karabeyoğlu v Turkey App no30083/10 (ECHR, 2016)

Klass and Others v Germany App no 5029/71 (ECHR, 1978)

Kruglov and Others v Russia App no 11264/04 and 15 (ECHR,2020)

Kvasnica v Slovakia App no 72094/01 (ECHR, 2009)

Liberty and Others v UK App no 58243/00 (ECHR, 2008)

Malone v The United Kingdom App No 8691/79 (ECHR, 1984) para 87

Roman Zakharov v Russia App no 47143/06 (ECHR, 2015)

Rotaru v Romania App no 28341/95 (ECHR, 2000)

S and Marper v The United Kingdom App no 30562/04 and 30566/04 (ECHR, 2008)

Slivenko v Latvia App no 48321/99 (ECHR,2003)

Silver and Others v the United Kingdom App no 5947/72 (ECHR, 1983)

Tyrer v The United Kingdom App no 5856/72 (ECHR, 1978)

International Treaties

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)

European Treaties

Charter of Fundamental Rights of the European Union [2000] OJ 1 364/1

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981 European Treaty Series No. 108)

Secondary Resources

Books

Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, And The Future of Law Enforcement (1st edn, New York University Press 2017)

David Bainbridge, Introduction to Information Technology Law (6th edn, Pearson Longman 2008) 636

Lawrance Lessig, Code: Version 2.0 (2nd edn, New York: Basic Books 2006)

Reed, C., 2004. Internet Law. 2nd ed. Cambridge University Press, pp.1-2,128.

Stephen B Wicker, Cellular Convergence and the Death of Privacy (1st edn, Oxford University Press 2013) 55

Contributions to edited books

Nidhi Rastogi, WhatsApp Security and Role of Metadata in Preserving Privacy. in Bryant and others (eds), Proceedings of the 12th international conference on cyber warfare and security (Academic Conferences and Publishing International Limited 2017) 269

Journal articles

Colin Crawford, 'Cyberplace: Defining a Right to Internet Access Through Public Accommodation Law' [2004] 76(2) Temple Law Review 225-276

Daragh Murray and Pete Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' [2019] 52(1) Israel Law Review 31-60

Elizabeth Goitein, 'Another Bite out of Katz: Foreign Intelligence Surveillance and the “Incidental Overhear” Doctrine' [2018] 55(1) American Criminal Law Review 105-125

Frederic Zuiderveen Borgesius and Wilfred Steenbruggen, `The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust` [2019] 19(2) Theoretical Inquiries in Law 291-322

John Naughton, 'The evolution of the Internet: from military experiment to General Purpose Technology' [2016] 1(1) Journal of Cyber Policy 5-28

Jon Penney, 'Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study' [2017] 6(2) Internet Policy Review 1-39

Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' [2013] 3(4) International Data Privacy Law 222-228

Michael A Epstein and Stuart D Levi, 'Protecting Trade Secret Information: A Plan For Proactive Strategy' [1988] 43(3) The Business Lawyer 887-91

Jarvie, 'Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1' [2003] 9(3) Computer and Telecommunications Law Review 76-81

Perry Keller , 'The Reconstruction of Privacy through Law: A Strategy of Diminishing Expectations' [2019] 9(3) International Data Privacy Law 132-152

Peter Swire, 'Efficient Confidentiality for Privacy, Security, and Confidential Business Information' [2003] Brookings-Wharton Papers on Financial Services 273-310

Purtova Nadezhda, 'The law of everything Broad concept of personal data and future of EU data protection law' [2018] 10(1) Law, Innovation and Technology 40-81

Riana Pfefferkorn, 'Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?' [2017] 49(5) Connecticut Law Review 1393-1452

Robert E Endeley, 'End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger' [2018] 9(1) Journal of Information Security 95-99

Robert Graham, 'How Terrorists Use Encryption' [2016] 9(6) CTC Sentiel

Samuel Warren and Louis Brandeis, 'The Right to Privacy' [1890] 4(5) Harvard Law Review 193-220

Stefan Schuster and others, 'Mass surveillance and technological policy options: Improving security of private communications' [2017] 50 Computer Standards & Interfaces 76-82

Yasir Gokce, 'The Bylock fallacy: An In-depth Analysis of the Bylock Investigations in Turkey' [2018] 26 Digital Investigation 81-91

Online journals

Joss Wright, 'Necessary and inherent limits to internet surveillance' [2013] 2(3). Internet Policy Review, <https://policyreview.info/articles/analysis/necessary-and-inherent-limits-internetsurveillance> accessed 13 March 2020

William Mciver and others, 'The Internet and the right to communicate' [2003] 8(12) First Monday <https://doi.org/10.5210/fm.v8i12.1102> accessed 19 June 2020

Websites and blogs

Comey James, 'Encryption, Public Safety, and "Going Dark"' (Lawfare, 6 July) <https://www.lawfareblog.com/encryption-public-safety-and-going-dark> accessed 02 August 2020

Digital Europe, 'Encryption: finding the balance between privacy, security and lawful data access' (Digital Europe, 16 March 2020) <https://www.digitaleurope.org/resources/encryption-finding-the-balance-between-privacy-security-and-lawful-data-access/> accessed 15 August 2020

Federal bureau of investigation, 'Going Dark' (Federal Bureau Of Investigation's website, 2016) <https://www.fbi.gov/services/operational-technology/going-dark> accessed 01.06.2020

Federal bureau of investigation, 'Lawful Access' (Federal Bureau Of Investigation's website) <https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch/lawful-access> accessed 01.06.2020

Jim Baker, 'Rethinking Encryption' (Lawfare, 22 October 2019) <https://www.lawfareblog.com/rethinking-encryption> accessed 18 August 2020

Lei Xu and others, 'Information Security in Big Data: Privacy and Data Mining' (IEEE , 09 October 2014) <https://ieeexplore.ieee.org/abstract/document/6919256> accessed 27 July 2020

Peter Swire, 'The Golden Age of Surveillance' (Slate, 15 July 2015) <https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html> accessed 21 August 2020

Riana Pfefferkorn, 'The earn it act: how to ban end-to-end encryption without actually banning it' (The Center for Internet and Society at Stanford Law School, 30 January) <http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it> accessed 30 August 2020

Tim Cook, 'A Message to Our Customers' (Apple, 16 February 2016) <https://www.apple.com/customer-letter/> accessed 09 August 2020

UK Home Office, 'Forensic Information Database Service (FINDS): International DNA and Fingerprint Exchange Policy for the United Kingdom' (UK Government, 8 July 2019) <https://www.gov.uk/government/publications/international-dna-and-fingerprint-exchange-policy-for-the-uk/forensic-information-database-service-finds-international-dna-and-fingerprint-exchange-policy-for-the-united-kingdom> accessed 13 July 2020

Whatsapp, 'Bringing Payments to WhatsApp for People and Small Businesses in Brazil' (WhatsApp Blog, 15 June) <https://blog.whatsapp.com/bringing-payments-to-whatsapp-for-people-and-small-businesses-in-brazil> accessed 29 August 2020

Whatsapp, 'Making WhatsApp free and more useful' (WhatsApp Blog, 18 January) <https://blog.whatsapp.com/making-whats-app-free-and-more-useful> accessed 02 July 2020

Whatsapp, 'WhatsApp Encryption Overview Technical White Paper' (*Whatsapp*, 2016) <https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf> accessed 19 June 2020

Newspaper articles

Ahmed Azam and David D. Kirkpatrick, 'Hacking a Prince, an Emir and a Journalist to Impress a Client' (The New York Times, 31 August 2018)

Andrew Sparrow, 'WhatsApp must be accessible to authorities, says Amber Rudd' (The Guardian, 2017)

Carole Cadwalladr and Emma Graham Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (The Guardian, 17 March 2018)

Charles Duan and others, 'Policy approaches to the encryption debate' (RStreet, 5 March 2018)

Dipesh Gadher, 'London Bridge terror attack planned on WhatsApp' (The Times, 2019)

Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' (The Guardian, 6 June 2013)

Ismet Karakas and others, 'Turkey: 18 FETO terror group suspects held' (Anadolu Agency, 21 July 2020)

Jeff Horwitz, 'As WhatsApp Tops 2 Billion Users, Its Boss Vows to Defend Encryption' (The Wall Street Journal, 12 February 2020)

Nicholas Watt, Rowena Mason and Ian Traynor, ‘David Cameron pledges anti-terror law for internet after Paris attacks’ The Guardian (Brussels, 12 January 2015)

Paul Tassi, 'How ISIS Terrorists May Have Used PlayStation 4 To Discuss And Plan Attacks [Updated]' (Forbes, 14 November 2015)

The Economist, 'Thieves in the night' (The Economist's website, 17 December 2014)

The Economist, 'The world’s most valuable resource is no longer oil, but data' (The Economist's website, 6 May 2017)

Others

Article 29 Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (WP 258, 29 November 2017)

Article 29 Working Party, ‘Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU’ (Brussels, 11 April 2018)

Article 29 Working Party, 'Working Document on surveillance of electronic communications for intelligence and national security purposes' (WP 228, 5 December 2014)

Council of the European Union, ‘Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)’ COD (2017/0003)

David Anderson, 'A Question of Trust' (UK Government, June 2015) <https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review> accessed 01 August 2020

David Anderson, 'Report of the bulk powers review' (UK Government, 19 August 2016) <https://www.gov.uk/government/publications/investigatory-powers-bill-bulk-powers-review> accessed 01 August 2020

ECHR, 'Background paper for the Judicial Seminar 2020: The Convention as a Living Instrument at 70' (*ECHR*, 2020) <https://www.echr.coe.int/Documents/Seminar_background_paper_2020_ENG.pdf> accessed 12 August 2020

ECHR, 'Factsheet on Mass Surveillance' (September 2019) <https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf> accessed 10 June 2020

Senate committee on the judiciary, 'Going Dark: Encryption, Technology, And the Balance Between Public Safety and Privacy' [2015] One Hundred Fourteenth Congress, First Session