*Mikayil Shaldiyev**

GOVERNMENTS' LEGAL ACCESS METHODS TO ENCRYPTED COMMUNICATION (CRYPTOGRAPHY): COMPARATIVE ANALYSIS

Abstract

Hiding text technique was used since early stages of history. After the governments of many states authorized and protected individuals in using encryption, more and more threats began to accompany the society. The governments figure out the ways in dealing with pre-crimes and minimizing the committed crimes made through encryption in future. Some found effective ways of dealing with cryptographic communication while some found hard to tackle with the problem through the law they have made. This article interprets the levels of legal access to ciphertext in different jurisdictions.

Annotasiya

Mətn gizlətmək texnikası tarixin erkən dövrlərindən bəri istifadə edilmişdir. Hökumətlər bütün şəxslərə şifrələmədən istifadə etməyə icazə verdikdən və şifrələmələri müdafiə etdikdən sonra cəmiyyətdə daha çox təhlükə müşahidə olunmağa başlandı. Hökumətlər gələcək üçün şifrələmə ilə edilmiş cinayətlərin qarşısını almağın və sayını azaltmağın yollarını axtarmağa başladılar. Bəziləri kriptoqrafik ünsiyyətlə mübarizə aparmağın effektiv yollarını müəyyən edə bildilər, digərləri isə ərsəyə gətirdikləri qanunlar vasitəsilə şifrəli ünsiyyətlə mübarizə aparmaqda çətinlik çəkdilər. Bu məqalədə müxtəlif yurisdiksiyalarda şifrəli mətnə hüquqi girişin səviyyələri təfsir olunub.

CONTENTS

* Baku State University, LL.M on Information Security Law.

Introduction

Encrypting information has begun since ancient Egyptian era. Mathematically encrypting data origins from XIX century when communication was mainly made telegraphically. During that time, it was forbidden among most European nations to encrypt data except for governments. Unidentified language was regarded as a code and bound for interrogation. Beginning from 1865 individuals were allowed to send encoded messages.[1] First encryption was used through internet for military purpose. Later on, telecommunication industries joined the networking industry to be part of this tendency.[2]

Hazardous encrypted communication once was less researched area by the U.S. federal government, however, cryptography was on their surveillance until now.[3] As reported continuous threats occurred through encrypted communication, government reacted upon it by establishing ways of obtaining information legally. It might seem easy at first sight, nonetheless, if certain data is encrypted, it requires additional procedures of decrypting it by obtaining relevant cryptographic keys.[4] If communication is encrypted, it is impossible to identify the sender and the receiver. Doubtlessly, this "metadata" collected by the government is significant in different kinds of operations.[5]

Federal government believes that encryption of communication will be significant problem for the law enforcement authorities in the future.[6] Unfortunately, they have predicted it right. Due to recent bombings in Brussels, several politicians, including German and French ministers said, law enforcement authorities need access to data information of any kind to prevent forthcoming crimes.[7] According to formal statistics, more than half of cybercrimes committed within EU, was via use of encrypted language. Around half of Member states stated an increase in use of encrypted email. Encrypting text is certainly vital for confidentiality of individuals, yet at the same time, it is an issue for law enforcement authorities to depict a criminal of any sort.[8]

[1] Kevin McArthur and Christopher Parsons, Understanding the Lawful Access Decryption Requirement, 7. (2012). Available at SSRN: https://ssrn.com/abstract=2148060
[2] Hilarie Orman, Encrypted Email the History and Technology of Message Privacy, 14 (2015).
[3] Adam Young, Moti Yung, Malicious Cryptography Exposing Cryptovirology, xxiii. (2003).
[4] Computer Science and Telecommunications Board National Research Council, Cryptography's Role in Securing the Information Society, Washington, D.C.: National Academy Press, 79 (1996).
[5] Orman, *supra* note 2, 47.
[6] *Supra* note 4, 87.
[7] EU Cybersecurity Agency Slams Calls for Encryption Backdoors (2016), https://www.euractiv.com/section/digital/news/eu-cybersecurity-agency-slams-calls-for-encryption backdoors/ (last visited November 16, 2018).
[8] The Internet Organised Crime Threat Assesment (IOCTA), The Hague: The EUROPOL Police Office, 50 (2015).

Notwithstanding, there are also counter-arguments against government's access to encrypted data. Technological industries prioritize that allowing government's seizure of information would damage the trust of their clients. For example, in EU data holders state that it will violate the privacy rights of EU citizens.[9] We will tend to identify perspectives of different governments in relation to privacy rights.

I. Introducing cryptography

Definition and utilization purposes of cryptography

Cryptography is a field in technical science that teaches us principles, methods and sources of hiding information. Moreover, cryptography assists us in prevention of unauthorized utilization and secretly changing of data. An individual can cover the real content of information with different methods in hardware, computers and communication channels by cryptography.[10] This sphere of science is part of cryptology which deals upon either securing or violating confidentiality with certain algorithms. Cryptanalysis is the second branch of cryptology in which its mechanism characterizes as offensive. Hackers, virus creators and other maliciously acting users violate information safety of cyber world by cryptanalysis.[11]

More precisely, cryptography uses various techniques to turn obvious text into cipher text. In process of encrypted communication, authorized access to the encoded text is made by the help of encryption keys known to the sender and the receiver.[12] Initially, cryptography has been used in military intelligence, diplomacy and state intelligence for covering the communication. Additionally, cryptography mainly used in money transactions, cash card safety and electronic signatures. The mutual aspect of all utilizations is to prevent third parties from interfering.[13] For example, when buying a product online, encryption ensures the transaction made by the credit card is bound to be safe.[14] Best example of encrypted communication is emailing process.[15]

[9] *Supra* note 7.
[10] Vəli Qasımov, İnformasiya təhlükəsizliyin əsasları, 132-133 (2009).
[11] Malicious Cryptography, Part One (2006), https://www.symantec.com/connect/articles/malicious-cryptography-part-one (last visited November 4, 2018).
[12] William Stallings, Cryptography and Network Security Principles and Practices, 32 (4th ed. 2005).
[13] Uses of Cryptography, https://www.digit.in/technology-guides/fasttrack-to-cryptography/uses-of-cryptography.html (last visited November 4, 2018).
[14] McArthur and Parsons, supra note 1, 2.
[15] Orman, supra note 2, 3.

II. Practices in various jurisdictions

A. EU perspective

Following the recent Paris and Brussels attacks head officials of certain Member States raised their concerns prior to the issue on personal data. Precisely, for safety reasons, law enforcement agencies should have legal privileges for obtaining information in order to prevent potential human disasters. [16] Europol ex-director Rob Wainwright said: "Encrypted communication via the internet and smartphones are a part of the problems that investigators face." He emphasizes potential dangers of encrypted text that is found in cell phones or other electronic gadgets of terrorists and other type of criminals, if not interfered by investigating agencies.[17]

Generally speaking, government access to encrypted communication is regulated on EU Member State level. EU approaches to the case with the soft law which is the 2001 non-binding resolution on cooperating with telecommunication firms in assistance of investigating encrypted data. The reason is that EU agencies and Member States have not reached mutual consent on accessing hidden private information. The argument goes about whether prioritizing privacy rights comparing to society safety rights would be reasonable, if they contradict each other.[18] In the resolution, it gives right to a Member State enforcement agency to request a telecommunication company to provide certain encrypted communication in a given time period.[19] Moreover, it authorizes a state official to obtain subject's identity, service number or other distinctive identifier by the help of a telecommunication firm.[20]

According to treaty on the functioning of the European Union, there are 2 conditions in legally solving cases – exclusive and shared. Exclusive is when authority is granted only to EU in dealing with certain matter, whereas shared competence is either EU or an EU Member State has right to mutually bind acts.[21] Information security falls upon shared competence.[22] If we consider there is no single consensus among EU executive departments, some Member States will use this opportunity to fulfil the security gap.[23]

---

[16] Government Access to Encrypted Communications (2016), https://www.loc.gov/law/help/encrypted-communications/index.php (last visited Nov. 11, 2018).
[17] How Europe Can Get Encryption Right (2016), https://www.politico.eu/article/how-europe-can-get-encryption-right-data-protection-privacy-counter-terrorism-technology/ (last visited Nov. 4,2018).
[18] *Supra* note 16.
[19] Council Resolution on "Law enforcement operational needs with respect to public telecommunication networks and services", 6-9 (2001).
[20] *Supra* note 19, 12.
[21] "Consolidated Version of the Treaty on the Functioning of the European Union", Brussels: Eur-lex Official Journal C 326, art. 2, 2012.
[22] *Id.* art. 4.2.
[23] *Supra* note 16.

There is no any binding resolution on EU level that requires telecommunication firms assist in giving out encryption keys for ciphered communication.

B. The UK perspective

The UK has abrupt legislature for obtaining encrypted information. Investigatory powers bill promised for law enforcement agencies right to have an access to encrypted data by forcing entities.[24] If terms are fulfilled, Regulation of Investigatory Powers Act 2000 gives permission to people with statutory power to have an access to encrypted communication by providing a notice to a person. The purposes are mainly characterized as preventing or detecting crime and the interests of the economic well-being of the UK.[25] If person refuses to obey, he becomes guilty of an offence such as imprisonment.[26] Investigatory Powers Act 2016 transmits even more power to law enforcement agencies. The Secretary of State issues warrants for obtaining encrypted information from an individual.[27] The reasons of law enforcement agencies and intelligence services to appeal to get a warrant are: (i) national security interest, (ii) detecting or preventing serious crime, (iii) interests of the economic well-being of the UK.[28] Judicial Commissioner also has an authority of obtaining information from a telecommunication operator by an approved notice.[29] If cipher text owner domiciled in Scotland, then Scottish Ministers has a right to issue a warrant for an official. [30]

Obligation for assistance by operators is mentioned in clause 128 of the Act 2016.[31] Foreign interference can also be made by the request of the head of an intelligence service to the Secretary of State.[32]

III. Local practice

Azerbaijani perspective

In Azerbaijan, law enforcement agencies have extensive authority in accessing encrypted text. They can either have permission to obtain information by a court order or conditionally obtain themselves.[33] Normally, the process of acquisition begins with interrogator's appeal to a court for a permission order. Government official, who carries out an investigation, can annex data by his order only if he completes his task, he presents his order to

[24] *Supra* note 7.
[25] Regulation of Investigatory Powers Act, Sec 49. (2000).
[26] *Id.* Sec. 53.
[27] Investigatory Powers Act, Sec 20. (2016).
[28] *Id.* Sec.19.
[29] *Id.* Sec. 53.
[30] *Id.* Sec. 21.
[31] *Id.* Sec. 128.
[32] *Id.* Sec.138.
[33] Criminal Procedure Code of Azerbaijan Republic, art. 445.2 (2000).

a supervisory court and procurator no later than 48 hours.[34] Moreover, the content of a crime case should concern either specifically a dangerous national security offense or a grave crime against a person.[35] Furthermore, officials who carry out the operation should be characterized as staff of the procurator office dealing against corruption.[36] These also include National security and intelligence agencies of Azerbaijan.[37]

Telecommunication companies have obligation to assist the government officials on supplying surveyed encrypted communication.[38] Moreover, they need to keep the given information confidential, especially when providing to national security and intelligence agencies.[39] It is considered as a crime, if telecommunication companies create obstacles to interrogators.[40] Sanctions include a penalty equivalent between 600 and 3000 dollars or up to 3 years of job disposal or up to 1 year of imprisonment.[41] Obstacles consist of refusing to obey an order, ignoring to provide technical condition such are equipment and devices for obtaining data of any sort.[42]

Despite the telecommunication companies have obligations on providing information, there is no obvious provision in legislation of Azerbaijan on assisting the government in decrypting data. The phrase "provide necessary condition" can enhance debates between telecommunication companies and law enforcement agencies.[43]

Conclusion

As described in the article, encryption can be used by any person in nowadays. However, allowing use of encryption and providing its protection have led to threats and factual disasters in the world. Therefore, EU confirms that the matter should be regulated in the Member State level.[44] Due to different approaches in various countries on accessing encrypted data, unions like EU could not come up with binding solution. If we analyze the whole text, we determine that the governments mainly get authorized access to ciphertext in purpose of preventing dangers against national security and interrogating grave crimes against a person. Investigatory Powers Act 2016 gets criticized by many scholars, because it eases law enforcement agencies' access to encrypted data and even allows them to hack computers by

[34] *Id.* art. 445.
[35] Detective-Search Activity Act of the Republic of Azerbaijan, art. 10 (1999).
[36] *Supra* note 32, art. 5.
[37] Law on Intelligence and Counter-Intelligence, art. 8 (2004).
[38] Law on Telecommunication of Republic of Azerbaijan, art. 33 (2005).
[39] *Supra* note 34, art 17.
[40] Criminal Code of Azerbaijan Republic, art. 233-3. (1999)
[41] *Ibid.*
[42] Firudin Samandarov, Commentary of Criminal Code of Republic of Azerbaijan, 627-628 (2009).
[43] *Supra* note 37.
[44] *Supra* note 21.

themselves.[45] Therefore, it weakens the trust between a customer and a telecommunication entity. On the other hand, it blocks forthcoming national and international terrorist attacks beforehand. In Azerbaijan, during an investigation process, encrypted data is obtained normally by an interrogator's appeal to a court for an order of obtaining. Despite this, Azerbaijan also hands wide range of rights to the government officials on accessing data, nevertheless, there is no obvious article or rule in legislation of Azerbaijan that obligates a telecommunication company to assist a law enforcement agency official on decrypting encrypted communication. Thus, we propose an obvious article in the Criminal code of Azerbaijan stipulating:

"noncooperation of a telecommunication company on decrypting data in means of averting dangers against national security and preventing serious crimes."

[45] The Snooper's Charter Shows the Government's Total Contempt for Privacy (2016), https://www.theguardian.com/commentisfree/2016/mar/01/proposed-snoopers-charter-shows-governments-contempt-for-privacy (last visited December 1, 2018).