Moritz Konarski, 27.11.2019 – New Mass Media

Facebook Messenger and the Debate about Encryption

In March of 2019, Mark Zuckerberg, the CEO of Facebook, wrote a blog post detailing the future he envisions for the platform. Currently Facebook is a digital "town square" that allows people to connect with friends and communities publicly, but now users increasingly want to communicate privately, in a digital "living room". Zuckerberg further explains that a digital "living room" requires private messaging and an all-around privacy-focused network and Facebook – not always known for its privacy as Zuckerberg remarks – intends to build that in the near future. In order to build a privacy-focused network, two main features are needed: strong encryption and reduced permanence (Zuckerberg, 2019). Strong encryption ensures that no one except for the intended recipient can read a message, while reduced permanence means that data and messages will be deleted after a period of time, making sure that they are not misused. Facebook plans to implement these reasonable privacy features across their messaging platforms, most notably Facebook Messenger.

Concerning privacy, the European Commission states in their *Eleventh Progress Report Towards an Effective and Genuine Security Union* that "the use of encryption is essential to ensure cybersecurity and the protection of personal data" (2017, p. 8), a statement that is compatible with Facebook's approach. While Facebook focuses on communication between individuals, encryption has numerous other important applications where it protects personal data, including online banking, cloud data storage, and secure communication between a web browser and a website. Without encryption, none of these ordinary activities would be possible because the privacy and integrity of the data could not be guaranteed. Accordingly, encryption is one of the foundations of the modern internet and without it the internet would not exist like it does today.

Encryption can also have negative effects and this is made clear by an open letter sent to Mark Zuckerberg and Facebook in response to the above described blog post. In this letter from October 2019 the UK Secretary of State, US Attorney General, US Secretary of Homeland Security, and the Australian Minister of Home Affairs urge Facebook not to go forward with their plans to implement encryption on their messaging services because privacy should not be put above security. Their reasoning is that "Companies should not deliberately design their systems to preclude any form of access to content, even for preventing or investigating the most serious crimes" (Open Letter: Facebook's Proposals, 2019, p. 1) because encryption would also prevent Facebook itself from policing its service. The two main types of criminal content the officials are concerned about are terrorist content and child sexual exploitation and abuse. In 2018, Facebook reported 16.8 million instances of child abuse content, 70% of which are estimated to come from Facebook Messenger, which Facebook plans to encrypt. They also acted against 26 million pieces of terrorist content between October 2017 and March 2019 (Open Letter: Facebook's Proposals, 2019, p. 2). If all messages were encrypted, a large portion of this content could remain undetected, the perpetrators could elude punishment, and fewer crimes would be solved.

The problems that the use of encryption by bad actors, mainly terrorists, causes are also a concern for the European Union – especially for Europol. After terror attacks in Europe in 2014, 2015, and 2016, Europol and national law enforcement "pointed to encryption as a key threat and serious impediment to the detection, investigation, and prosecution of such criminal activity" according to *The Encryption Debate in the European Union* by Maria Koomen (2019, p. 1). The European Commission makes the same point in the *Eleventh Progress Report Towards an Effective and Genuine Security Union* (2017, p. 8), illustrating that encryption, while praised for its benefits by the Commission also poses a significant problem for law enforcement.

Encryption, like Facebook plans to implement it in Facebook Messenger, is described as both an asset and a liability, sometimes by the same organization. It is used to secure personal information, but this is often exploited by criminals. Because both the advantages and disadvantages are significant, a debate about the use of encryption has developed. This paper will give an overview of encryption, the debate in the EU, connect it to Facebook's proposal, and explore possible solutions or approaches to the issue.

To begin, encryption will be defined. Encryption is "a means of putting data in code. It allows people to transform a message or data into a form that can't be understood (decrypted) without knowledge of some secret information." (Baker, 1997, p. 729). In his paper *Decoding OECD Guidelines for Cryptography* Baker further describes that encryption is performed using a mathematical algorithm. A key is chosen and the algorithm uses it to encrypt the data or message, making it unreadable. When the message reaches its destination, the recipient applies the same algorithm and a key to decrypt it and makes it readable again (Baker, 1997, p. 730).

The debate about encryption in the EU needs to be seen in the context of previous debates on the issue because the EU debate is relatively young, having begun in 2016 (Koomen, 2019, p. 1), while encryption debates started in the 1990s (Abelson et al., 2015) or even earlier. The underlying issue is the same in all of these debates: the fear that law enforcement will not be able fight crime because criminals use encryption to hide their activity – this is sometimes called the fear of "going dark".

The fear of going dark is caused by the use of encryption that is unbreakable for law enforcement and thus keeps them from fighting crime. The underlying issue here is the balance between the user's right to privacy and the public's right to security. A proposed answer to this problem is the implementation of an exceptional access mechanism. This mechanism allows law enforcement agencies in certain situations and with the appropriate

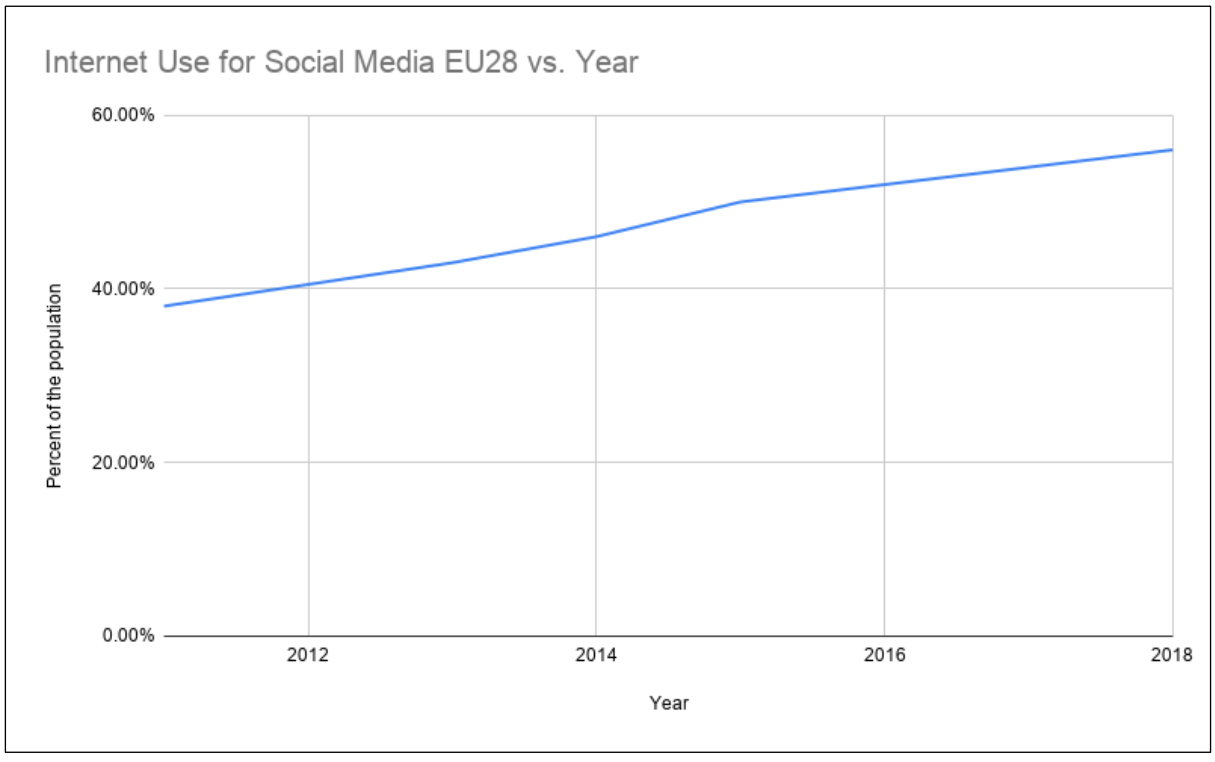
legal paperwork to access encrypted data. There are two main ways of designing exceptional access systems, each with their own problems.

On one hand, encryption can be designed to be purposefully weak, meaning it is easy to break. This can be achieved by restricting the length of the encryption keys, whose length is directly related to the strength of the encryption. The obvious problem with this approach is that encryption would not just be weak when criminals use it and law enforcement wants to break it, but in all circumstances. This would leave everyone vulnerable to attacks and be an asset to criminals. Additionally, criminals could simply chose not to use a service that has weak encryption and use one that offers strong encryption instead, making the weakening of encryption an ineffective tool of exceptional access.

On the other hand, encryption systems can be designed with backdoors that would allow law enforcement to access data without having to break the encryption itself, which would not weaken the encryption algorithm itself. A common variant of such a backdoor is the key-escrow system, where the key used for decryption is stored by a third party that can provide it to law enforcement when needed. But this approach has many problems which Abelson et al. outline in their paper *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communication* (2015). They state that implementing key-escrow systems would make security systems more complex and thus create more vulnerabilities in the process. When handling decryption keys there is the question of which agency handles them and that agency would then be a target for criminals because they hold the keys to a lot of private data. Criminals could again simply use services that do not participate in the key-escrow and make the system less effective. The authors conclude that key-escrow is not feasible because in addition to the mentioned problems it is highly complex, difficult to design and expensive to implement. As a result of both forms of

exceptional access having significant flaws, the debate has never really ended because no solution could be found.

A current example of this debate is the open letter the officials from the US, UK, and Australia sent to Facebook to convince them to implement some form of exceptional access into their system (Open Letter: Facebook's Proposals, 2019, p. 3) and while they do not provide any specifications for that system, it sounds like a key-escrow system which would have the problems outlined above. This conflict is important because social media and Facebook as its biggest platform play a huge role today. The following graph, based on EU Open Data Portal data about *Individuals Using the Internet to Participate in Social Networks* (2019), shows that over 50% of respondents use the internet to engage with social media and there is a growing trend. This illustrates the importance of this debate.

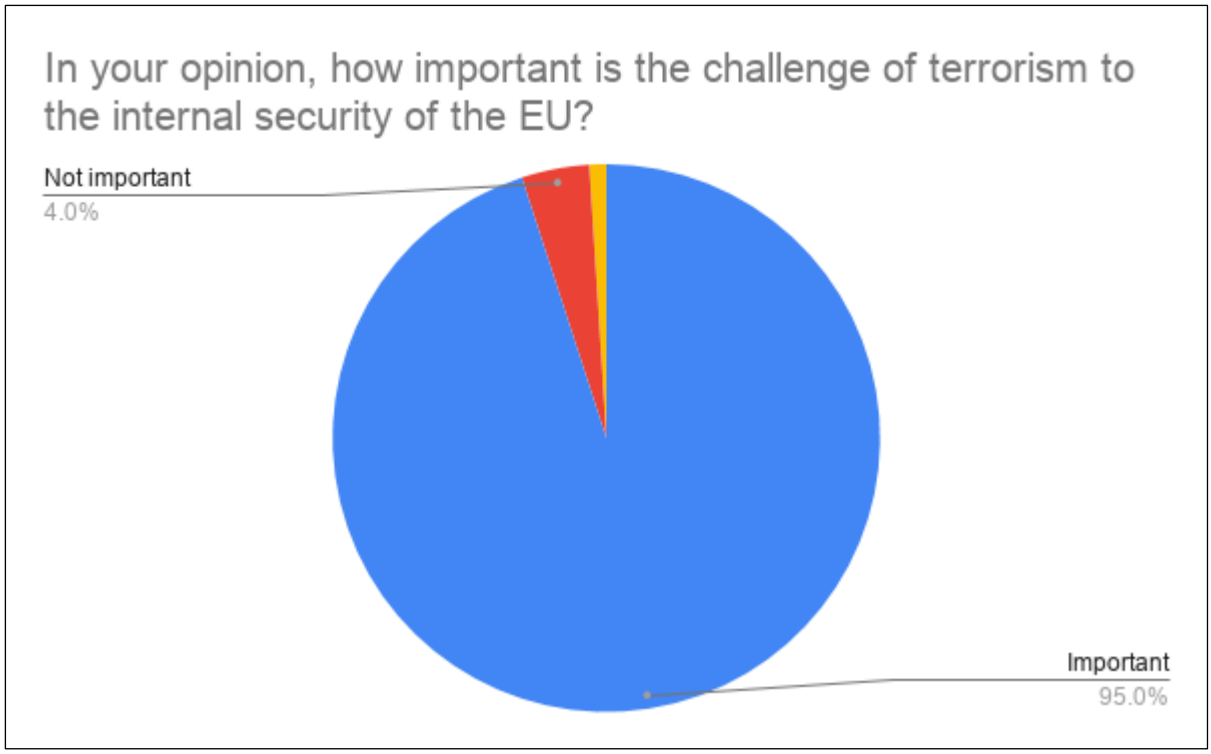


As the conflict between Facebook and the US, UK, and Australian government officials is still developing it is impossible to judge the outcome, especially because both sides have promised to work together to find a solution that satisfies all parties, but the conflicts between a proposed key-escrow system and Facebook's goals for privacy-focused networking can be

stated. Facebook wants strong encryption and reduced permanence, both of which are incompatible with a key-escrow system. Strong encryption cannot be broken and if there was a backdoor is would be significantly weakened, which would go against Facebook's plans to make Messenger secure and private. Reduced permanence adds to the problem by reducing the window of time in which the messages would have to be accessed before they are deleted. This would make it impossible to implement a working exceptional access system while maintaining the goals that Facebook set for their service.

The approach the EU has when it comes to encryption is different from the one proposed in the open letter, so it might offer a solution. In the EU, the debate on encryption is not concerned with exceptional access systems. The reason for this is that the European Commission explicitly states the importance of encryption and EU legislation notes its role as well (European Commission, 2017, p. 8). If the role of encryption is this clearly stated, it would be hypocritical to undermine it or to try to weaken it. Because the creation of backdoors is also problematic, Europol and the European Union Agency for Cybersecurity have come to the agreement to oppose backdoors for encryption services (Koomen, 2019, p. 3). As a result, the EU has to find alternatives to the two common ways of exceptional access that deal with the problems that encryption can pose.

After multiple terror attacks started the debate on encryption and law enforcement complained about encryption hindering their work, EU interior ministers met in 2016 to discuss the issue of encryption. This issue is also highly relevant for the European public, as a Eurobarometer from 2015 shows. The graph below is based on data from the EU Open Data Portal titled *Special Eurobarometer 423: Cyber security.* It shows that 95% of respondents think that terrorism is a challenge to the security of the EU. Terrorism as a driving force of the debate also sets it apart from the debate represented by the open letter to Facebook, where the main focus was child sexual exploitation instead.



After the meeting of interior ministers, France and Germany called for a "solution to encryption" and a questionnaire about the problems law enforcement has with encryption was issued (Koomen, 2019, p. 4). The questionnaire revealed a lack of technical expertise, cross-border cooperation, and funds to intercept communications that hindered law enforcement. The primary problem encryption caused was that evidence of crimes was hard to gather (Koomen, 2019, p. 5).

As a result, in a position from October 2017, the European Commission stated goals meant to alleviate the problems. Those statements were the result of consultations with experts on the subject and stakeholders like the European Agency for Fundamental Rights. The Commission reaffirmed the importance of encryption in the EU, but acknowledged that it negatively affects law enforcement's investigations. They conclude legal measures to enable access to encrypted evidence as well as measures to enhance decryption abilities (European Commission, 2017, p. 8). The legal measures are concerned with access to encrypted electronic evidence located in a different EU member state and funding for training for cross-border cooperation. The cooperation forms are also supposed to become standardized.

The technical measures are more extensive. The Commission wants to support member states in accessing encrypted information "without prohibiting, limiting or weakening encryption" (European Commission, 2017, p. 9). Firstly, they will support Europol to improve their decryption abilities by increasing its budget, particularly the European Cybercrime Center. Secondly, a "network of points of expertise" will be established that complements already existing national networks of expertise and is meant to increase knowledge sharing and cooperation. Thirdly, non-descript "alternative investigation techniques" should be developed to complement already existing techniques. Fourth, structured dialogue between law enforcement and industry and service providers will serve as the basis for better understanding of the whole issue. Lastly, training programs will be funded to improve law enforcements abilities to obtain encrypted information (European Commission, 2017, p. 9). In summary, all five points above aim to improve the abilities of law enforcement to decrypt encrypted evidence.

The approach the EU (more specifically the Commission) is taking on this issue is sidestepping the original problem of exceptional access that plagued the debates on encryption. They do this by reaffirming that encryption is important and that they are not trying to change that, instead they try to break the encryption anyways or look for alternative ways of accessing data that would be encrypted. Their ultimate goal here is the same as the one outlined in the open letter to Facebook –they want to access encrypted data to fight crime – but their approach is different. Instead of trying to weaken encryption to gain access and thus reducing the security of that encryption, the EU wants to scale up its abilities to break said encryption. This has the advantage over the other approach that it does not make encryption weaker for ordinary users and thus solves a big problem that exceptional access systems generally have.

While this approach works with Facebook's proposal to make Messenger more private, as it does not conflict with strong encryption or reduced permanence, there are some issues with it. First, strong encryption is very secure, even with improved capabilities it will not be easy for Europol or national law enforcement agencies to break it. The network of expertise might experience similar problems that already exist when it comes to the sharing of evidence. Furthermore, as the questionnaire by the interior ministers showed, the capabilities of member states vary a lot, meaning that even with cooperation there will still be big differences between them. One of the biggest issues is that the laws on state hacking or "alternative measures" are not very developed, meaning that this research and investment is being made without a proper legal framework (Koomen, 2019, p. 6-7). Most of these problems can be solved if there is enough political will behind it. Expertise networks and cooperation can be improved, even if that might take years, legal frameworks can and should be created to ensure legality, and the capabilities of member states could either be improved through targeted investments or by cooperation and sharing tasks with the countries that can solve them. The issue that cannot be solved is the strength of encryption, which the EU has little control over and here they have to engage in an arms race with cryptographers if they want to be able to break encryption effectively.

All in all, this approach seems to be more reasonable than the exceptional access approach that has more substantial problems. If the agencies can solve some of the potential problems of the EU approach outlined above, they might have found an acceptable solution to the issue of encryption. Not a perfect one, as encryption might just be too strong to break and because there is some irony to both supporting encryption and doing one's best to break it at the same time. In the future there will have to be some resolution to the Facebook Messenger conflict and it will no doubt have a big impact on the internet and private messaging as a whole, this development will be interesting to watch.

References

Abelson, H. et al. (2015). Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. MIT Technical Report

Baker, S. A. (1997). Decoding OECD guidelines for cryptography policy. *The International Lawyer, 31(3), p. 729-756*

Open Letter: Facebook's Proposals. (2019). Retrieved from https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg

Koomen, M. (2019). The Encryption Debate in the European Union. Carnegie Endowment for International Peace

EU Open Data Portal. (2019). *Individuals Using the Internet to Participate in Social Networks*. Retrieved from https://data.europa.eu/euodp/en/data/dataset/oY2vRJtab1L3kIb5T9flg

EU Open Data Portal. (2015). *Eurobarometer 423: Cyber security*. Retrieved from https://data.europa.eu/euodp/en/data/dataset/S2019_82_2_423_ENG

Zuckerberg, M. (2019). A Privacy-Focused Vision for Social Networking. Retrieved from https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/