Moritz Konarski, 14.10.2019
ES 236 - New Mass Media, Yulia Kalinichenko

Research Proposal: The Encryption Debate in the EU

There is a constant debate over the use of encryption on the internet and the ability (or lack thereof) of law enforcement to access data necessary to fulfill their duty. The problem is that modern encryption technology has become strong enough that it is not feasible to decrypt messages if one is not in the possession of the appropriate decryption key. While being great for privacy, it prohibits law enforcement agencies from investigating serious crimes, e.g. child sexual exploitation, terrorist activity or money laundering. A solution to this dilemma has yet to be found.

In the EU this debate has interesting facets. On one hand, Europol is claiming that encryption is one of the main obstacles they face in fighting crime on the internet. On the other hand, the European Commission has recognized encryption as a vital tool for protecting personal data, privacy, and freedom of expression. These two opposing views hint at the discord within the EU regarding this topic.

How can such opposing viewpoints come together to form a coherent EU policy? In an attempt to answer this question, this research will investigate the following sub-topics: the core of the encryption debate, the current state of this debate in the EU, and the existence of promising solutions.

The introduction will outline the basic issue of this research, use current examples to show its importance, connect it to the EU and contain the research question:

- Why is this debate important? It affects all online communication as well as real-world security
- How current is this topic? In October UK, US and Australian government officials sent a letter to Facebook asking them not to implement strong encryption on their services to allow the collection of data
- How does this relate to the EU? In the EU this debate has interesting facets. On one hand, Europol is claiming that encryption is one of the main obstacles they face in fighting crime on the internet. On the other hand, the European Commission has recognized encryption as a vital tool for protecting personal data, privacy, and freedom of expression.
- Research question: How can such opposing viewpoints come together to form a coherent EU policy?

The first section of the body will deal with the core of the encryption debate. Here, a short history of the debate around encryption will be given, the fundamental issue(s) shown, and it will be shown why this debate has not been settled yet:

- What is the history of this debate? In the 1990s there were the “Crypto Wars” which ultimately did not change the way encryption is used, but started a lot of discourse
- What are the issues? There seems to be no right answer when the privacy of everyone is weighed against the chance to detect criminals. Also, there is no easy way to just weaken privacy when crime is being fought

The second section of the body will give an account of the current developments and status of the encryption debate in the EU:

- What is the current status? There are conflicting statements by different EU bodies regarding the debate. The capabilities of member states to deal with encryption as well as the legal frameworks vary wildly. Some countries are pushing for EU legislation around this issue. Some countries have more problems with encryption when fighting crime than others.

The final section of the body of the paper will look at whether there are any solutions for the debate in the EU in sight:

- What solutions have been proposed? The implementation of backdoors to encryption has been largely ruled out. It is proposed to improve law enforcement's capabilities to break encryption. Others propose to evade encryption by e.g. accessing data before it is encrypted. The sharing of information between EU member countries is planned to be increased and simplified.

The conclusion will state the answer to the proposed research question.

- Are there any solutions to the encryption debate in sight? This remains to be seen, it will be the result of the research. It does appear that there is still no solution everyone could agree to.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W.,...Weitzner, D. J. (2015). Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. MIT Press

ENISA. (2016). ENISA Threat Taxonomy. Retrieved from https://data.europa.eu/euodp/en/data/dataset/enisa-threat-taxonomy-1

EU Directorate-General for Communication. (2017). Special Eurobarometer 464a: Europeans' attitudes towards cyber security. Retrieved from https://data.europa.eu/euodp/en/data/dataset/S2171_87_4_464A_ENG

Europol. (2017). European Union Serious and Organised Crime Threat Assessment 2017. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

Europol. (2019). First report of the observatory function on encryption. Retrieved from https://www.europol.europa.eu/publications-documents/first-report-of-observatory-function-encryption

Europol. (2019). INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Koomen, M. (2019). The Encryption Debate in the European Union [PDF]. Retrieved from https://carnegieendowment.org/files/WP_The_Encryption_Debate_in_the_EU.pdf

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/