Mattia Danese
CS 183: Privacy in the Digital Age
Professor O'Brien
Assignment 2

Encryption Memo

Ever since the turn of the 21st Century, encryption and encryption policy has come to the forefront of privacy and privacy legislation. In short, encryption, or the act of encrypting information, is when data is cryptographically modified in such a way that its meaning is no longer decipherable to anyone other than the intended recipient. The backbone of modern encryption algorithms are very complex mathematical problems (i.e. modular exponentiation) which are *impractical* to break. Thus, it is very clear why encryption, in today's Digital Age, is integral to individual and societal privacy: encryption gives an individual the power to have their secrets remain secret. With such a powerful tool being publicly available and usable, governing bodies across the globe have approached encryption policy in varying ways. The European Union (EU) is one governing body to note, and its encryption policies, along with its more general privacy policies known as the General Data Privacy Regulation (GDPR), are renowned for being fairly strict and having a great focus on accountability across corporations and governments [6]. In this memo, the development, current standing, and possible future states of encryption policy in the EU will be further analyzed.

The origins of the encryption debate in the EU date back to the first Crypto War in the mid-1990s. The first Crypto War was sparked by US export controls which limited the availability and usability of encryption software. Under these export controls, encryption software was intentionally weakened by imposing limits on encryption key sizes. Additionally, the US Bureau of Industry and Security had the authority to grant licenses to individual bodies which enabled the export of encryption software to them; those who were denied a license were

only able to receive weaker encryption software [1,2,3]. The US justified its export controls as a means of national security; however, problems started to arise when these controls inevitably spilled over to the global economy and other governments. As such, privacy advocates rallied against this legislation under the notion that it was a violation of the human right to privacy and an impediment to economic growth [4]. Moreover, advocates questioned the legal and moral implications of a governing body accessing encrypted data and limiting the power of encryption available to its citizens and non-citizens [3]. Many credit privacy advocates for "winning" the first Crypto War, as the internet is flowered with end-to-end encryption; but, following terrorist attacks in 2016, the EU revisited these debates with a focus more towards counter-terrorism. Now in the second Crypto War, the stance of privacy advocates remained unchanged, but the opposing stance regarded strong encryption as being a shield for criminals and enabling "perpetrators to mask their identity" [5].

Due to the anonymization of the internet, made widely possible by encryption, the current environment of encryption policy in the EU has reached a stalemate. On one hand, EU legislation labels encryption as a means to achieve "an appropriate level of security for the protection of fundamental rights and data". On the other hand, numerous politicians view encryption as a possible gateway to crime and a direct cause to officials' inability to curb the stark increase in child pornography, terrorist attacks, and other crimes across Europe over the past decade [5]. That being said, there have been numerous attempts by EU officials to find a balance between private sector security and the ability to circumvent encryption during criminal investigations. For example, in the summer of 2020, the European Commission proposed new legislation which would mandate companies to scan encrypted and unencrypted content of their users for child pornography. However, the European Parliament later shot down this proposal as

it “did not live up to EU privacy rules” [5]. Shortly afterwards, the at the time German Presidency of the Council of the European Union called for a collaboration between policy makers and the tech industry. Leaving this sort of threat detection up to corporations may lead to a slippery slope, as seen with the efforts of Apple in August of 2021. On the flip slide, such collaboration may also be a step in the right direction as Seny Kamara, an expert in cryptography, notes that some companies have made it possible to unencrypt online messages, to then report to law enforcement, if illegal content was shared [5]. At the moment, it is clear that encryption policy in the EU has hit a back-and-forth between two dire, but also conflicting, interests: protecting the human right to privacy and the ability to convict and prevent criminal activity.

Moving forward, the EU will need to make multiple important decisions regarding its encryption policy. First and foremost, the EU will need to hone in on where the line is drawn between protecting privacy and its appropriate exceptions. The European Commission is once again working on its previously mentioned legislation, though it may face the same fate barring any substantial changes to how users get vetted for unsolicited scanning of their data [5]. Another decision the EU will have to make, that is not explicit legislation, is how encryption is defined and portrayed to the public. Diego Naranjo, a privacy advocate, interestingly states that the portrayal of encryption and scanning content “as a dilemma between child protection and privacy is a false dichotomy” [5].

The approach of the EU with regards to its encryption policy is one of many. It is known for being stern and focused on protecting a person’s data, and in turn rights, rather than government and corporation liberties. EU encryption policy originated through advocating for wide public use of encryption, but now more so regards pinpointing the equilibrium between

personal security and bringing forth justice. In terms of the future, technology, encryption, and the need for privacy will inevitably continue to evolve which makes the encryption and privacy policies of the EU, or any other entity for that matter, far from being set in stone.

References

[1]O'Brien, David. (2023, February 27). Encryption and Encryption Policy [PowerPoint slides]. The Fletcher School, Tufts University. https://www.dropbox.com/scl/fo/ug7ck4d8xbo8cbne06udq/h?dl=0&preview=Week_6_Encryption_and_Encryption_Policy.pdf&rlkey=ql6o48qghj6md1egtv353jqty

[2]O'Brien, David. (2023, March 6). Encryption and Compelled Assistance [PowerPoint slides]. The Fletcher School, Tufts University. https://www.dropbox.com/scl/fo/ug7ck4d8xbo8cbne06udq/h?dl=0&preview=Week_7_Encryption_and_Compelled_Assistance.pdf&rlkey=ql6o48qghj6md1egtv353jqty

[3]Soesanto, S. (2018, July 5). *No middle ground: Moving on from the crypto wars*. ECFR. Retrieved from https://ecfr.eu/publication/no_middle_ground_moving_on_from_the_crypto_wars/

[4]Ranger, S., Staff, T. R., Azhar, A., Branscombe, M., Hughes, O., Miles, B., & Greenberg, K. (2015, March 12). *The Undercover War on your internet secrets: How online surveillance cracked our trust in the web*. TechRepublic. Retrieved from https://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/

[5]Koomen, M. (2021, March 31). *The encryption debate in the European Union: 2021 update*. Carnegie Endowment For International Peace. Retrieved from https://carnegieendowment.org/2021/03/31/encryption-debate-in-european-union-2021-update-pub-84217

[6]*What is GDPR, the EU's new Data Protection Law?* GDPR.eu. (2022, May 26). Retrieved from https://gdpr.eu/what-is-gdpr/