Zelalem Yitbarek
CS-285L P-03 Professor A. Potasznik

Social Issues and Ethics In Computing Final Paper: Long Weekly Write-Up Version

Privacy constitutes the majority of online users' concern when an individual or organization send, receive, or access information through the internet. Everyone wants to make sure that the information is safe; that a third party is not accessing data, especially if the information or data has a sensitive nature like financial, health or national information. While studying this issue, computer scientists invented an end-to-end data encryption system. This system translates the sent information into an unreadable code along with an encrypted key. Only the legitimate receiver of the information has this unique key. They are then able to decode and open the data. If for any reason, such code falls into the wrong hands before it gets to the receiver, it is nothing more than an irrelevant gibberish document. Giant tech companies implement this service in their products, such as Google and Facebook. Facebook uses this security method on WhatsApp and Instagram(Perlroth). Although this end to end data encryption guaranteed users online communication privacy, it shuts down the backdoor access for law enforcement. It then becomes a huge obstacle for law enforcement to prevent and defend the criminal and terrorist acts. For the purpose of this paper, I nominate myself as a Judge to oversee this case, and I will apply ethical principles to decide whether tech companies redesign end-to-end encryption to enable back door access.

On one hand, the Justice Department is arguing that "end-to-end encryption makes it much harder to track terrorists, pedophiles, and human traffickers" (Perlroth). This claim implies that without having backdoor access, it is hard to ensure private citizen safety and security. It sounds like a legitimate claim because it is evident that terrorists and organized criminals widely used online communication platforms to conduct violent missions. In order to stop and bring them to justice, law enforcement needs to investigate these online communications. Otherwise, law enforcement can not efficiently prevent crime and protect citizens without the power to access information from multiple sources. It is apparent that information is life to any intelligence operation; without enough and relevant information, their operation becomes inefficient and irrelevant. If inefficiency happens, it can have adverse effects on society in two aspects. One, it put millions of lives in danger; two, it is a misallocation of taxpayer money and resources. For example, the Utah Datacenter would pay $3.3 million on electricity bills for nothing each month(Potasznik, Day 5). if all collected data were unable to decrypt; they could not be able to lead to criminals or terrorist doorsteps.

On the other hand, tech companies claim that they should protect the privacy of their customers. "Apple's chief executive, Timothy D.Cook, who believes people should be able to have online communications free of snooping" (Perlroth). Hence end-to-end data encryption makes such privacy policy and believes in free communication by prohibiting backdoor access of intelligent authority. On top of that, it protects users' information from hackers. So that **KEY ASPECTS OF PRIVACY** would fulfill, freedom from surveillance and freedom from intrusion(Potasznik, Day 4). Hence people and businesses feel safe and secure while they conduct online communication. Many might agree with this statement since privacy is a crucial part of an individual and organization. So this security system will protect people's privacy and safety.

This controversial issue has a potential impact on at least four stakeholders, users, intelligent authority, tech companies, and hackers. First, individuals and businesses refer to users, want information privacy, as well as safety and security. Practically it is hard to fulfill these demands at the same time. So that end-to-end encryption would have a double-edged sword effect on them. Users, individually, will benefit by having Information privacy, devoid of spying, and hacker threat. However, as a society, the risk would be their physical safety and security because law enforcement would not be able to protect them due to a lack of relevant information. If law enforcement as granted backdoor access, the user will benefit since they will be secure and safe, but they risk their privacy since agents can look at their information. Unethical officers might use it for personal benefit, which would leave room for conflict of interest. Second, Intelligence Agencies want to have the legal power to access online communication through a backdoor. Having such power will give them the ability to tackle criminal activities and preserve national security. Third, tech companies want to have a reliable security system that is devoid of backdoor access and hackers.

Implementing such a system will help tech companies to build a good reputation that leads to make them much money. End-to-end encryption also has the potential to damage their reputation because criminals and terrorists use the platform for their evil mission. Mark Zuckerberg said, "Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things" (Perlroth) So, people and government point their finger at tech companies and raise a moral issue, but not legal. Of course, they are not legally accountable for their user's illegal activity. **TELECOMMUNICATIONS ACT OF 1996**, part two; title V, section 230, states that "no provider of interactive computer services shall be treated as a publisher of any information provided by another information content provider." (Potasznik, Day 6). This law ensures that tech companies are not responsible for their user's data communication content even though the end-to-end encryption protected criminals' privacy as well. However, it might have a chance to prompt lawmakers to come up with a bill that forces the tech company to back up from such a system or allow back door access. Lastly, unethical hackers want to steal and devour users' information for the sake of either political or financial goals. If a tech company forced to hand over the master key (backdoor access allowed), it will be a golden opportunity for hackers. For any reason, when they get the key, they would own the entire population data. However, end-to-end encryption would have the potential to prevent such action.

There are various law interpretations that deal with stakeholders and backdoor access. For users, end-to-end encryption does not allow backdoor access, which alines with **The FOURTH AMENDMENT**, which is unreasonable searches and seizures. Moreover, the **title II Stored Communications Act**: restricts government and business access to e-data (Potasznik, Day 5). These two laws explicitly prohibit backdoor access (unreasonable searches). However, law enforcement can use the following law interpretations, **COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA) 1994** requires telecom equipment to be designed to ensure that the gov't can intercept telephone calls (Potasznik, Day 5). Amended Electronic Communications Privacy Act (ECPA) includes electronic communications(Potasznik, Day 5). So According to this law, tech companies require to redesign end-to-end encryption in a way law enforcement is able to intercept online communications. Besides, there is another legal support, **Section 702** of The Foreign Intelligence Surveillance Act (FISA), which explicitly allowed mass warrantless surveillance(Potasznik, Day 5).

One option would be allowing law enforcement back door access. By doing this, they would have relevant information that bestowed them the ability to prevent criminal activities ahead. So that people will live in a safe and secure environment. It would happen at the expense of mass privacy. In this case, the risk and disadvantage of the back door outweigh its benefits. One, not all people engaged in criminal and terrorist activity; only a few of them are out there. It is not rational to spy on entirely innocent people. Second, criminals or terrorists cannot attack all citizens, and only a few people could be victims. Third, there is no guarantee for the security of massive collected data; hackers could steal it. Four. The collected data potentially could be abused or manipulated by politicians or corrupted intelligent agents for personal interest. Due to these reasons, this option does not offer the most benefit to the majority of people. It does not meet the **UTILITARIANISM** expectation, which is for the greater good.

The second option would be to decline backdoor access. In this way, people's private information will be kept private and devoid of snooping and hacking. In such a way, people would exercise their fundamental constitutional rights. One, since they have no fear or concern about their online communication security, they can communicate and express their ideas freely. It is an example of the **First amendment.** Second, their online privacy only searched or decrypted on the presence of a warrant, which means this tech security system creates a suitable environment to protect them from unnecessary search and seizure that is the fourth amendment. The massive drawback of this option is national security and people's and business safety because this technological loophole creates an excellent opportunity for criminals and terrorists to conduct harmful activities on people and national security. But it protects users and national security from cybercriminals.

Although the second option has a downside, it has substantial benefits and constitutional law support. As mentioned above, end-to-end encryption is like a technological or technical version of the fourth amendment because it prohibits unreasonable search of data or invasion of electronic communication by the third-party. One of the third party are law enforcement who gather data and spy on innocent people for the sake of crime fight. CALEA and section 702 give them legal power. This legal loophole widely opens the door for conflict of interest. "The FBI illegally wiretapped the phones of Americans, often falsely invoking terrorism emergencies" (Potasznik, Day 5). So, end-to-end encryption would not allow this to happen since data decryption is impossible. Hackers also try to invade private, business, and government privacy and become a threat to national security. However, end-to-end encryption makes them less threatening. In this case, such an encryption system help national security to be healthy by protecting and securing individual, health, financial, and government sensitive transit date. In conclusion, end-to-end encryption should be implemented without granting backdoor access.

Work Cited

Potasznik, Amanda. Spring 2019, CSIT285L. Day 5 slides. Retrieved from https://cpb-us-w2.wpmucdn.com/blogs.umb.edu/dist/7/3673/files/2018/05/Day-5-2fehnts.pdf on May 11, 2019.

"What Is End-to-End Encryption? - The New York Times." 19 Nov. 2019, https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html. Accessed 12 Dec. 2019.