Ethics about Encryption

Victor Delaplaine

CPE 329, Cal Poly

Should companies be forced to add a mechanism to allow governments or law enforcement to access the encrypted data quickly?

I think they should. But firstly, the government should review its privacy and protection laws to ensure there is a balance between privacy and national security. National security precedes everything, given the recent mass shootings and ever-increasing terror threats (Comey, 2014). Take, for instance, the San Bernardino attack that occurred in December 2015 (Bay, 2017). The FBI was unable to unlock Mr. Syed Rizwan Farook's iPhone and asked Apple for help (Bay, 2017). In my opinion, this request should have been treated as an exemption. Mr. Syed had been proven to be one of the attackers and probably posed a more serious threat to national security even in death. Accessing his iPhone would have helped the FBI in further investigations since it was reported that it looked as though they had planned the attack. Besides, a third suspect was captured. Undoubtedly, accessing their iPhones would have unearthed more into the attack.

Should companies that put hard encryption (that which cannot be accessed or decrypted easily) in products or services be held responsible if bad actors (criminals, terrorists, etc.) use their product or service to commit crimes?

No, I think it would be wrong to hold an entire company responsible for another person's misdeeds. Data protection laws are stringent and thorough. Their breach, if proven, could have severe consequences. Therefore, companies that put hard encryption on their devices are only adhering to the data protection laws to avoid the effects. Victimizing them is wrong. However, it is the national government's responsibility to ensure the existence of a balance between privacy and national security. The balance will eliminate a haven for criminals to operate, and companies will be obliged to decrypt the criminals' communication data.

If people have nothing to hide, they should have nothing to fear with possible government surveillance of their “encrypted” communication. Do you agree or disagree?

I disagree. I think privacy should be respected. For instance, I do not think anyone would be comfortable with the government accessing their texts or photos, health records, financial data, and locations. Even in government, if such data falls in the wrong hands, it could be used to harm the individual. Besides, there is no guarantee that the government's access to such data will be limited to surveillance and criminal investigation purposes only. In my opinion, privacy is paramount, and I can only show you what I want to. However, for proven criminals, the case should be different. For them, their encrypted data should be put to scrutiny as this would help in investigations and possibly avert planned criminal activities.

References

Bay, M. (2017). The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone. *First Monday*, *22*(2). Retrieved from http://journals.uic.edu/ojs/index.php/fm/article/view/7006

Comey, J. (2014). Going dark: Are technology, privacy, and public safety on a collision course?. *US Department of Justice*. Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course