End-to-End Encryption, Good or Bad?

Josh Smith

CYBR-3310.203

Sunday Ogunlana

4/29/2023

End-to-End Encryption (E2EE) is one of the most relevant topics to modern day cryptography, where the people's right to privacy and law enforcement's oath to protecting the people clash. This study takes on the challenge of identifying why there is an issue, what possible solutions exist, and if this ordeal affects end users at all. This case study takes the opinion that everybody has the right to use E2EE without the government interfering. To support this stance, this study will present three arguments in favor of E2EE as well as a rebuttal to a common counterargument. There is one assumption to be made before this case study is carried out: that the policies suggested and laws referenced only apply to the United States of America. Many of the topics covered will be applicable to other countries and governments, but, for the sake of simplicity, all positive statements and opinion-based judgements will pertain to the context of American law.

The first argument that this study poses in favor of consumer E2EE is that removing criminal's ability to communicate via E2EE channels does not stop criminals from communicating secretly. Just by making E2EE illegal will not deter criminals because they are already willing to commit crimes. Additionally, E2EE is trivially easy to set up at any layer of the network communication stack (also known as Open Systems Interconnection—or OSI—model). For example, an IP connection may not be secured, but the parties can communicate securely as far down as the Transport layer using Transport Layer Security (TLS) and as high up as the Application layer using custom software. If E2EE services are banned, hackers and criminals will not be the group that suffers. Instead, innocent people's private conversations and data will be exposed to Internet Service Providers (ISPs), who seek to sell consumer data to advertisers, and cybercriminals, who are always looking for an unencrypted channel of communication to intercept.

Secondly, in Katz v. United States, the Supreme Court ruled that if somebody expects and is confident in the privacy of an instance of communication, then the Fourth Amendment protects them from law enforcement-initiated eavesdropping (such as wiretapping). The purpose for which law enforcement agencies seek to petition the end of E2EE may be entirely invalid under this law because forcing a reasonably private channel of communication into plain view is essentially modern-day wiretapping. Because companies are not required or instructed on how to store customer data (Etzioni, 2016), there will be no data to provide to the government since messaging is ephemeral. Additionally, prosecutors have the ability to obtain a warrant for the private keys to be used in decryption, which makes it entirely unnecessary for

Lastly, there is a concept referred to as the "Hydra Effect" where implementing partial solutions causes problems to manifest elsewhere in ways worse than the original. In the context of this study, this could mean that by preventing communication via E2EE, bad actors can and will come up with more obscure alternatives to hiding criminal activity. As previously stated, E2EE can be implemented on almost any layer of the OSI model, so the bad actors can simply buy or design encryption tools that work at the application layer. Building an E2EE messaging app is as simple as googling "how to write an end to end encryption app," which brings up Jain's simple step-by-step, "E2EE for beginners" blogpost (Jain, 2021). Additionally, modded messaging apps can be sideloaded onto Android and jailbroken iOS devices. Cybercriminals are, by definition, more technically advanced than the average consumer, so building tools and sideloading apps are trivial tasks. All this to say, by taking away consumer E2EE, the government outright revokes the people's rights to privacy and incentivizes criminal organizations to design more complex encryption alternatives.

Now, some people may say that there is a compromise between banning consumer E2EE and allowing it, which is that E2EE can be implemented in such a way that the government will have backdoor access. This argument seems valid and effective on the surface, but once analyzed, it is evident that this is one of the worst solutions. Implementing a backdoor into E2EE conversations means that they are no longer truly "end-to-end" encrypted; instead, they become "end-to-end plus third party" encrypted, which not only sounds less secure but indeed is. Given enough time, hackers can and will find a way to access a backdoor, and Abelson et al. words it perfectly, "Providing access over any period of time to thousands of law enforcement agencies will necessarily increase the risk that intruders will hijack the exceptional access mechanisms." Additionally, given the uproar surrounding the E2EE debate, the hackers will immediately know when to start looking for a backdoor if this "solution" is implemented. Even if the backdoor is not found for years, people's data is still vulnerable due to "Store Now; Decrypt Later" (SNDL). This cannot be emphasized enough: law enforcement does not benefit enough from disabling or modifying E2EE to outweigh the threat posed towards innocent people and their right to privacy—not only from the government, but also bad actors.

In conclusion, this study has argued and supported three major points in favor of the persistence of end user's right to encrypt as well as refute a common counter argument against this. If the contents of this study have failed to persuade the reader to change their opinion, or—at the very least—provide plenty of information on the state of the debate, then hopefully this excerpt from a technical report by MIT's Computer Science and Artificial Intelligence Laboratory will leave an impact:

> We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago.

> In the wake of the growing economic and social cost of the fundamental insecurity of today’s Internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force Internet system developers to reverse “forward secrecy” design practices that seek to minimize the impact on user privacy when systems are breached. (Abelson, et al. 2015)

By taking away consumer E2EE, the government simply takes power and rights away from the people and incentivizes criminal organizations to design more complex encryption alternatives.

Sources Cited

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. A., & Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and Communications. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyv009

Endeley, R. E. (2018). End-to-end encryption in messaging services and national security—case of WhatsApp messenger. Journal of Information Security, 9(01), 95.

Etzioni, A. (2016). End to End Encryption, the Wrong End. South Carolina Law Review, 67(3).

Jain, V. (2021, January 12). Developing a real-time secure chat application like WhatsApp & Signal with end-to-end encryption. QED42. Retrieved April 29, 2023, from https://www.qed42.com/insights/coe/javascript/developing-real-time-secure-chat-application-whatsapp-signal-end-end

Katz v. United States, 389 U.S. 347 (1967)