End-to-End Encrypted Messaging Services Are Here to Stay Even with Government Interference

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Rithik Yelisetty
Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature Rithik Yelisetty Date 05/07/2021
Rithik Yelisetty

Approved _____ Date _____
S. Travis Elliot, Department of Engineering and Society

Abstract

Internet messaging services have adopted a new standard to increase the security and privacy of messages sent on their platform: end-to-end encryption. End-to-end encryption ensures that only intended individuals can view the contents of messages, keeping conversations private from governments, data collection companies, and other users. This paper will utilize the Social Construction of Technology (SCOT) framework to analyze the role of end-to-end encryption and how governments have interfered in the spread of this technology. The analysis section details all of the major social groups (users, governments, and platform operators) and their associated views on end-to-end encryption technology. The discussion section discusses possible solutions that can be implemented to appease the government's concerns regarding this technology. As a result of the analysis and discussion, readers will be able to understand the vitality of end-to-end encryption and why it will continue to exist regardless of any government interference.

Introduction

Communication via internet services has become increasingly more prevalent due to the ubiquity of technology in everyone's daily lives. The only proven method to keep messaging content sent via these platforms secure from the outside world is to utilize end-to-end encryption methods. End-to-end encrypted (E2EE) platforms encode messages on the sender's device so that only the intended receiver can decode the message to understand the contents. This ensures that any unintended recipients, including any middlemen like governments or the platform operators themselves, cannot decipher the contents of messages.

This paper will analyze government interference in end-to-end encrypted messaging platforms through the lens of the Social Construction of Technology (SCOT) STS framework by focusing on evaluating how humans directly impact the development and usage of technology in society. The SCOT framework is analyzed primarily through the concept of interpretative flexibility, entailing that technology and its associated social factors must be considered through the perspective of relevant social groups. This paper will also examine the tension between the three relevant social groups (users, governments, and platform creators), and how they each view E2EE services, in addition to providing possible solutions to help end-to-end encrypted services stay prominent despite concerns by governments.

Background

End-to-end encrypted systems have become some of the most popular communication methods in today's connected world, some of the most common being WhatsApp (owned by Facebook) and iMessage (owned by Apple). WhatsApp is an application that is available on both iOS and Android, along with web and native desktop clients, and ensures that users only need an active internet connection to send and receive messages. The availability of WhatsApp on all

platforms has propelled the application as a global leader in the messaging industry and has allowed the platform to grow exponentially to over two billion active users, growing by over five hundred million active users in just two years (Porter, 2020a). iMessage, the other popular encrypted messaging service, works solely across the Apple ecosystem, consisting of iPhones, iPads, and Macs, and is preinstalled on all of these devices. Due to the ease of access, iMessage has grown rapidly in the US and has introduced features like video calling and interactive games. The rapid growth of these services has led to a heightened concern amongst government officials, as they no longer have methods of conducting messaging data collection operations to reduce crimes, terrorist-related activities, child-sex exploitation, and misinformation.

Analysis: Understanding the Battle of End-to-End Encrypted Chat Services

This paper will view current government interference into end-to-end encrypted standards by using the Social Construction of Technology (SCOT) STS framework. SCOT was initially developed by Wiebe Bijker and Trevor Pinch, both of whom were professors of the STS departments at their respective universities, through their article "The Social Construction of Facts and Artefacts" ("Trevor J Pinch" n.d.; "Wiebe Eco Bijker" n.d.). The SCOT framework is based entirely on how humans can shape technology – not the other way around. This is in opposition to other STS frameworks like Actor-Network Theory, where the two-way relationship between how technology and human action shape each other is evaluated. The SCOT framework revolves around three primary principles: relevant social groups, interpretive flexibility, and closure and stabilization (Rosen, 2002, p.15).

Users, Governments and Platform Operators: The Perspectives from Relevant Social Groups

As described in the original article written by Bijker and Pinch, the concept of relevant social groups entails that there are several groups of individuals that have different perspectives

on how technologies should impact society. Bijker and Pinch (1984) describe that the main idea of this concept is that every member of a certain social group must have the same belief (p. 414). In terms of end-to-end encryption, there are three primary social groups: users, governments, and platform operators. Everyday users value the use of end-to-end encryption as they believe that their messaging data should remain confidential and should not be accessed by any external entities. This is confirmed by a Pew Research Center survey that claimed that over 90% of adults believe that they should have control over who can view their personal data (Madden & Rainie, 2015). In addition, a survey conducted by Reuters shows that users believe that their messaging data is the most private data of all data collected by internet companies. The survey also indicated that more than three-fourths of respondents would rather use end-to-end encrypted services to keep their data private instead of using unencrypted messaging services to allow the US government to comb through all messaging data to prevent terror plots (Volz, 2017). Similarly, privacy advocates have raised concerns about user messaging data being shared with advertisers to better serve targeted advertisements. As one of the most personal forms of communication, platforms can learn more not only about who an individual is messaging but also about an individual's purchasing habits, locations of interest, and ideologies. This, in turn, leads to these corporations earning more revenue per user, without any added benefit for their users. Privacy advocates have claimed that this is a blatant violation of the users' data privacy rights as users do not have the option to opt-out of sharing data with platforms.

Governments, on the other hand, want to restrict the use of end-to-end encryption as this technology prevents them from collecting data vital to stopping crime and terrorism-related incidents (Graham, 2016). The US Government has previously tried to eliminate the risks associated with E2EE platforms by forcing companies to implement backdoors, or secret

methods for governments to view and collect data, in their software using programs like the PRISM program led by the National Security Agency (NSA). For example, the government mandated Microsoft to build a method to conduct surveillance operations on warranted individuals in their end-to-end encrypted messaging platform, Skype (Endeley, 2017). By allowing for surveillance to be conducted on Skype, the government believed that they would be able to stop acts of violence against their citizens specifically since data was collected in secrecy. More recently, governments across the globe have tried pleading with companies, like Facebook, publicly to implement this backdoor technology, maintaining their viewpoint that they would not be able to protect their citizens against imminent attacks ("International Statement: End-To-End Encryption and Public Safety", 2020).

Companies are seemingly stuck in a middle ground – offering end-to-end encryption helps improve their public perception and win privacy-related legal cases but could potentially deteriorate their relationship with governments, leading to their platforms being banned in certain regions (Wall & Musotto, n.d.). In court cases, platforms seemingly have an easy excuse for claiming that they were unable to report incidents since they cannot read individual messages. On the other hand, governments, like the Chinese government and the North Korean government, have banned applications like WhatsApp due to the fact that they do not explicitly share communication data with them (Bradsher, 2017). In addition, companies that choose against implementing end-to-end encrypted messaging can benefit by collecting additional data about their users to help earn supplemental revenue through targeted advertisements. According to a study published by researchers at the University of Texas at Austin, the Fortune 1000 companies could increase revenues by an average of 10% by effectively collecting and using customer data to better understand products that need to be created (Barua et al., n.d., p. 3). This

can be extrapolated to messaging platforms – platforms can help improve their products and can better serve ads to their customers. They could also collect data regarding how people view other products and pass feedback to companies to help them further innovate.

Interpretations and Stabilizing Ideas regarding End-to-End Encryption

The second tenet of the SCOT framework, interpretive flexibility, entails that individuals or groups can interpret concepts differently (Rosen, 2002, p.15). Bijker and Pinch (1984) describe this concept with the example of the Hill Report theorizing that the sun oscillates through a range of frequencies. Several scientists were unable to confirm Hill's hypothesis, making it seem like his assumption had been proven wrong. The authors, however, describe how this represents interpretive flexibility, as nature itself "does not force the issue" but rather human action shapes these ideas (p.420). In the case of end-to-end encryption, the Earn It Act can be used as an example. The Earn It Act tries to prevent end-to-end encryption by forcing the providers of chat services to monitor and report child exploitation (Graham, 2020). In the view of lawmakers, this bill can stop child sexual exploitation by forcing the companies that operate these chat services to report these instances to the government. This would, in turn, give the government the ability to prosecute individuals for these crimes. As a side benefit, lawmakers may view the passage of the Earn It Act as a way to introduce further legislation to require platforms to look for instances of violence or terrorism in an effort to reduce these types of incidents. From the view of users and the messaging providers, this would require a full stoppage on end-to-end encrypted messaging platforms to ensure that the messages being sent are not in violation of this law. Since companies would be required to complete analysis on each message sent via their platform, they would be required to have the ability to read every message and would therefore no longer maintain the status of being an end-to-end encrypted platform. Experts

in this field have also claimed that the Earn It Act will expedite the movement of individuals from mainstream platforms to other custom-built platforms, where data is channeled through regions that the US government has no jurisdiction over (Pfefferkorn, 2020). This would result in the US government losing the ability to gain any knowledge on messaging data, in addition to users (both guilty and innocent individuals) migrating to non-American services that protect their data. This would result in American corporations losing out on significant revenues.

The third concept of closure and stabilization can be explained as an idea that is agreed upon by all of the relevant social groups and is eventually taken for granted (Rosen, 2002, p.15-16). In terms of end-to-end encryption, all of the relevant social groups (users, governments, and platforms) involved concede that users require a messaging platform that is more secure and private than the current non-E2EE messaging services available. For example, Facebook, the operator of three of the largest messaging platforms (Messenger, Instagram, and WhatsApp), has even announced that they plan to convert all of their existing messaging platforms into one fully end-to-end encrypted service showing that they understand that their users want a more secure and private solution to messaging ("Hard Questions: Why Does Facebook Enable End-to-End Encryption?", 2018; Isaac, 2019). Governments around the globe have also attempted to implement measures that layout requirements regarding user data storage. In the European Union, the General Data Protection Regulation law, more commonly known as GDPR, requires companies to collect minimal amounts of user data, improve data protection security and store user data for only a specified amount of time ("What is GDPR, the EU's new data protection law?", n.d.). Laws like GDPR can be used to prosecute companies to reduce misuse of data and can improve overall user trust in both technology companies and governments. E2EE systems abide by GDPR laws as companies do not have the ability to collect messaging data on users and

therefore do not have to worry about data storage location. Governments have also passed legislation entailing strict data residency requirements to ensure that any data collected by companies does not leave certain regions and is not scoured by foreign entities.

Another idea that is agreed upon among all of these groups is that the amount of misinformation and illegal content sent via messaging platforms must be restricted. Given that platforms do not have the ability to read messages, platforms have taken the stance of not blocking any message from being sent. However, the ability to forward messages has been restricted by platforms like WhatsApp in order to slow the spread of messages. According to WhatsApp, the removal of the forward button for messages that have been forwarded too many times has led to a 70% reduction in the spread of viral messages, many of which are considered misinformation (Porter, 2020b). These measures can help improve the quality of message content received by platform users and can make platforms safer as a whole.

Discussion

End-to-end encryption is here to stay despite strong opposition from governments around the world. Billions of users have already migrated to using end-to-end encrypted technologies and this phenomenon was further accelerated during the protests against police brutality in June 2020. Protestors claimed that law enforcement agencies were using StringRay technology in cities like New York City, giving them the ability to collect cellphone data, like messaging and calling data, without the knowledge of individual cellphone users (Neirenberg, 2020; Goldstein, 2016). Protestors worried that law enforcement agencies would retaliate against individuals participating in the protests despite not committing a crime. This led to a mass migration to end-to-end encrypted services, like Signal, which noticed an over 400% increase in app downloads in

the span of one week. By using these E2EE services, users felt safer as StringRay technology could not be deployed to gather information about the protest's participants (Neirenberg, 2020).

E2EE services were first developed in the early 1990s in the form of PGP encryption and since then, the technology has been heavily used in messaging applications. Since the encryption technology required for E2EE has been released to the public in an open-sourced format, governments no longer have the ability to stop individuals from creating their own applications that operate using this technology. This means that if the US government were to block major E2EE services like WhatsApp or iMessage, other individuals or corporations could release a new application that is fully end-to-end encrypted. In addition, these new applications could be developed and released in countries that are not allied with the United States (like Russia), essentially blocking the government from implementing any regulations or surveillance measures to actively help reduce issues like child-sex exploitation and terrorism-related incidents.

Addressing Governmental Concerns with End-to-End Encryption

The US government, however, has several options in order to help reduce the risks associated with E2EE messaging services. First, the government could require companies like Facebook and Apple to implement client-side filters to detect child-sex exploitation efforts, the main area of concern addressed by the Earn It Act. Platforms could be required to ask users for their date of birth to determine whether adult content can be sent or received by the user. If the user is not over a certain age, platforms could use machine learning techniques combined with computer vision in order to detect whether an image contains adult content and prevent that message from being spread. Similar machine learning techniques can also be used to sift through text messages to detect instances of this type of exploitation. These detection mechanisms could run on the user's application, rather than on central platform servers, to maintain the platform's

end-to-end encryption promise. The government could go a step further and require platforms to report multiple-offense users in an effort to accomplish the goals set out by the Earn It Act. Messaging services currently do not implement this technology due to the high costs of development combined with an unwillingness to "censor" user messages. Services might be concerned that users will migrate to other platforms due to the perceived sense that their messages are no longer end-to-end encrypted if certain messages are blocked from being sent.

To combat misinformation, governments can force platforms to implement similar machine learning techniques on every message sent to determine if the message violates policies set forth (like those set on major social media platforms regarding the coronavirus), specifically those that could pose harm to users. If a message violates the regulations set forth, the message can either be reported to the appropriate authorities or removed altogether. By doing this, users are content to see that their messages are not discernable by external authorities and can rest easy that their messages do not violate any laws. Governments are satisfied that they can eliminate potentially dangerous messages from being sent and companies are willing to implement these measures to ensure that they are able to keep both governments appeased and users on their service.

Another solution that the US government could implement to restrict the use of E2EE platforms would be to require verification for individuals on these services. Prior to being allowed to send or receive messages, users would be required to submit valid government identification to be used for a background check, similar to the process of getting approved for TSA PreCheck or a government-issued REAL ID. The government would then be able to determine the likelihood of an individual using the service for malintent, whether that be for criminal-related offenses or otherwise. If government agencies like the FBI and the NSA

determine that the individual poses no likely threat to others, the government can issue an end-to-end encrypted verified ID, enabling a user to use any platform of their choosing. The government could improve this process further by completing continuous checks by working with local law enforcement authorities and national agencies to determine whether an individual should keep their approval. An issue with this approach might include the lack of wide adoption by platforms – if one platform forces individuals to have this government ID, users can choose to migrate to other services, which are custom-made or hosted outside of the US, to bypass this requirement.

Conclusion

End-to-end encryption has been adopted globally as the new standard for messaging and corporations are working on creating new products outside of the messaging realm that incorporate this technology. Users and privacy advocates view E2EE services as a reliable way to keep their messaging data secure, while platform providers view this technology as an easy solution to appease consumer fear that excessive amounts of data are being collected. Governments, however, view this encryption technology as a blockade from protecting their citizens against potential crimes and large-scale threats. The research discussed in this paper shows that banning end-to-end encryption is no longer a viable option as this technology has already been open-sourced and will lead to a mass migration away from American-operated services. Disallowing the use of end-to-end encryption will cause new technologies to emerge that emulate this behavior and will result in reduced privacy for users of messaging platforms. By passing new regulations that force platform operators to implement client-side filters for both child-sex exploitation and criminal activities, combined with a strict approval process for users, governments can continue to protect their citizens while enabling their citizens' right to privacy.

References

Barua, A., Mani, D., & Mukherjee, R. (n.d.). *Measuring the Business Impacts of Effective Data*. University of Texas at Austin. http://www.datascienceassn.org/sites/default/files/Measuring%20Business%20Impacts%20of%20Effective%20Data%20I.pdf

Bradsher, K. (2017, September 25). China blocks WhatsApp, broadening online censorship. *The New York Times*. https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html

Endeley, R. E. (2017). End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. *Journal of Information Security, 9*(1), 95–99. https://doi.org/10.4236/jis.2018.91008

Goldstein, J. (2016, February 11). New York police are using covert cellphone trackers, civil liberties group says. *The New York Times*. https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html

Graham, L. (2020, July 20). *S.3398—EARN IT Act of 2020* [Webpage]. https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

Graham, R. (2016, June 16). *How Terrorists Use Encryption*. Combating Terrorism Center at West Point. https://www.ctc.usma.edu/how-terrorists-use-encryption/

Hard Questions: Why Does Facebook Enable End-to-End Encryption? (2018, May 7). *About Facebook*. https://about.fb.com/news/2018/05/end-to-end-encryption/

International Statement: End-To-End Encryption and Public Safety. (2020, October 11). https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Isaac, M. (2019, January 25). Zuckerberg plans to integrate WhatsApp, Instagram and Facebook Messenger. *The New York Times*. https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html

Kumparak, G. (2014, February 27). Apple Explains Exactly how Secure iMessage Really Is. *TechCrunch*. https://social.techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/

Lee, C. (2018, March 8). *WeChat active accounts exceed 1 billion worldwide*. ZDNet. https://www.zdnet.com/article/wechat-active-accounts-exceed-1-billion-worldwide/

Madden, M., & Rainie, L. (2015, May 20). Americans' Attitudes About Privacy, Security and Surveillance. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Nierenberg, A. (2020, June 11). Signal downloads are way up since the protests began. *The New York Times*. https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html

Pfefferkorn, R. (2020, May 4). The EARN IT Act is a disaster amid the COVID-19 crisis. *Brookings*. https://www.brookings.edu/techstream/the-earn-it-act-is-a-disaster-amid-the-covid-19-crisis/

Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science, 14*(3), 399–441. JSTOR.

Porter, J. (2020a, February 12). *WhatsApp now has 2 billion users*. The Verge. https://www.theverge.com/2020/2/12/21134652/whatsapp-2-billion-monthly-active-users-encryption-facebook

Porter, J. (2020b, April 27). *WhatsApp says its forwarding limits have cut the spread of viral messages by 70 percent*. The Verge. https://www.theverge.com/2020/4/27/21238082/whatsapp-forward-message-limits-viral-misinformation-decline

Rosen, P. (2002). *Framing Production: Technology, Culture, and Change in the British Bicycle Industry*. MIT Press.

Rösler, P., Mainka, C., & Schwenk, J. (2018). More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema. *2018 IEEE European Symposium on Security and Privacy (EuroS P)*, 415–429. https://doi.org/10.1109/EuroSP.2018.00036

Silver, L. (2019, February 5). Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally. *Pew Research Center's Global Attitudes Project*. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

Trevor J Pinch. (n.d.). Cornell University - The Department of Science & Technology Studies. Retrieved October 12, 2020, from http://sts.cornell.edu/trevor-j-pinch

Volz, D. (2017, April 4). Most Americans unwilling to give up privacy to thwart attacks: Reuters/Ipsos poll. *Reuters*. https://www.reuters.com/article/us-usa-cyber-poll-idUSKBN1762TQ

Wall, D. S., & Musotto, R. (n.d.). *Facebook's push for end-to-end encryption is good news for user privacy, as well as terrorists and paedophiles*. The Conversation. Retrieved October 12, 2020, from http://theconversation.com/facebooks-push-for-end-to-end-encryption-is-good-news-for-user-privacy-as-well-as-terrorists-and-paedophiles-128782

What is GDPR, the EU's new data protection law? (2018, November 7). GDPR.Eu. https://gdpr.eu/what-is-gdpr/

WhatsApp Encryption Overview—Technical white paper. (2017). https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.

Wiebe Eco Bijker. (n.d.). NTNU. Retrieved October 12, 2020, from https://www.ntnu.edu/employees/wiebe.bijker