The Battle over End to End Encryption and The EARN IT Act

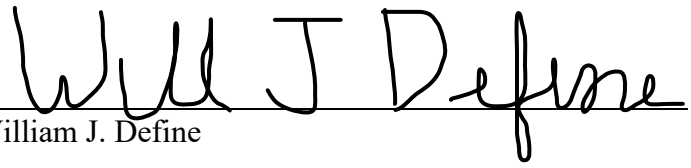
A Research Paper submitted to the Department of Engineering and Society

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

William J. Define
Spring, 2020

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  Date 4/19/20
William J. Define

Approved_____ Date_____
Richard D. Jacques, Department of Engineering and Society

Introduction

Over the past few years, various Law Enforcement and Government agencies have been sounding the alarm about End to End Encryption (E2EE). These officials worry that E2EE threatens public safety by making non-surveilable, unwarrantable encryption widely available to criminals, especially child predators. To many experienced technologists, their concerns sound familiar and dated. Law enforcement has complained about encryption since practically its inception. Take for instance FBI director Louis Freeh testifying in 1995:

> Powerful encryption is becoming commonplace. The drug cartels are buying sophisticated communications equipment. Unless the issue of encryption is resolved soon, criminal conversations over the telephone and other communications devices will become indecipherable by law enforcement. This, as much as any issue, jeopardizes the public safety and national security of this country (Freeh, 1995).

Freeh's concern is echoed more recently by Attorney General Bill Barr in 2019:

> Service providers, device manufacturers, and application developers are developing and deploying encryption that can only be decrypted by the end user or customer, and they are refusing to provide technology that allows for lawful access by law enforcement agencies in appropriate circumstances, (Barr, 2019).

The difference is the threat. Now, instead of the threat being the drug cartels, a concern of FBI in the 1990s, there is a focus on the threat of child pornography, the threat of the last decade. Barr warns "All companies, including Facebook, must have zero tolerance when it comes to child exploitation and not allow their platforms to facilitate these sick crimes" (Patel et al. 2019). The end result of the encryption deliberations in and since the 1990s has been to not interfere. Both the Government and tech companies think this is the right move. We face a similar tradeoff

today, but it is not clear the resolution will be in favor of encryption. On the one hand, bipartisan support in the Senate for the EARN IT Act have technologists and privacy advocates worried about a change in policy. Liberal democracies around the world such as the UK and Australia have taken steps towards banning E2EE. On the other hand, technologists, privacy advocates, civil libertarians, and ex-NSA chief Michel Hayden all remain in favor of E2EE (Hayden, 2015). E2EE opponents have countered the pro-encryption consensus with a much-improved villain in child predators and the vilification of the tech industry. They've channeled these forces into the EARN IT Act, a deceptive bill designed to thwart E2EE indirectly.

What is End to End Encryption?

Messaging uses public-private key encryption. That means each user has a public and private key. As their names suggest, the public key is widely shared while the private key is private. Data encrypted with one key, usually the public key, can only be decrypted with the other key, the private key. For instance, when Alice sends a message to Bob, Alice encrypts the message with Bob's public key, sends the encrypted message to Bob through a messaging server, and then Bob decrypts the message with his private key. This is E2EE. In non-E2EE messaging, the encryption happens twice: between Alice and the server and between the server and Bob. Therefore in a non-E2EE system, the server can read Alice's message to Bob.

A Short History of Encryption Battles

The battle over E2EE is only the latest in a decade's long history of encryption battles. The tactics of 2020 are an evolution of the tactics of the past. For instance, the idea of opposing encryption to stop criminals is found in the encryption battles of the 1990s. Similarly, the focus

on and vilification of tech companies heats up in 2016 with the Apple-FBI debate. Finally, the nineties battles led to CALEA and Section 230, two laws with heavy influence on encryption law and the EARN IT act today.

The Nineties: Criminals, CALEA, and Section 230

In the 1990's the US government first argued against encryption as a threat to prosecuting criminals. Law enforcement worried that strong encryption protected criminal communications even when law enforcement obtained a warrant. Louis Freeh, FBI director from 1993 to 2001, was one of the first to connect advancing encryption to protecting criminals. He testifies: "Uncrackable encryption will allow drug lords, terrorists, and even violent gangs to communicate with impunity. Other than some kind of key recovery system, there is no technical solution" (Freeh, 1997). The anti-encryption view was pervasive in government at the time. President Bill Clinton proclaimed: "We must combat an unholy axis of new threats from terrorists, international criminals, and drug traffickers" (Clinton 1998). In 2020, the criminals have shifted from the old "unholy axis" to child predators. Yet, the argument that encryption shields criminals remains.

The 1990's encryption debate informed two important laws today: CALEA, or the Communications Assistance for Law Enforcement Act, and Section 230 of the Communications Decency Act. CALEA forced telephone operators to redesign their network architecture to make government wiretapping easier. CALEA made two critical exemptions. It exempted internet services from adjusting their architecture and allowed for any communication platform to implement unwarrantable encryption. These exceptions enabled the proliferation of encryption on the web today (Pfefferkorn, January 2020). The 1990's also birthed Section 230 which laid

out critical protections for internet companies. These protections are the subject of the EARN IT Act.

2016: Apple vs FBI

In 2016, encryption opponents first set their eyes on big tech. In the aftermath of the San Bernardino terrorist attack, the FBI issued a court order for Apple to unlock the terrorist's iPhone. Apple declined. They reasoned that if they generated a key to unlock the phone, then that key would likely be released and everyone's privacy would be at risk (Cook, 2016). Law enforcement was furious with the decision. Here is Cyrus Vance Jr, Manhattan District Attorney: "Right now, they have independently struck a balance between privacy and public safety at that point on the spectrum where it coincides perfectly with their economic interests" (Vance 2016). In previous encryption battles, the enemy was nameless criminals. Now, the focus is on the tech companies as well. The companies are accused of unpatriotically not supporting law enforcement in order to protect their own economic interests. Problematically for encryption opponents in 2016, Apple had a mostly stellar reputation. In 2020, Facebook provides a much better foil.

Child Predators and Child Sex Abuse Material

In 2020, child predators replaced the criminals of the 1990's as the villain hiding behind encryption. It began in 2019 with a *New York Times* investigation of Child Sex Abuse Material (CSAM) that shocked the nation and inspired the EARN IT Act (Keller and Dance, November 2019). The report describes the CSAM problem in horrific detail. The stories of victims who must grapple with depictions of their assaults living forever on the internet are jarring. Worse still, the abusers of this material seem to face little pressure. These predators are well protected on the internet with strong encryption, vpns, and specialty dark web sites. Even with all this

protection, some CSAM is discovered. The National Center for Missing and Exploited Children (NCMEC) is the government funded agency responsible for reporting and handling CSAM online. NCMEC operates a CyberTipline for tech companies to report CSAM they find on their platforms. The growth and size of reports are astounding. For instance, last year NCMEC received 18.4 million reports containing 45 million images. This number is up from 1 million reports in 2014, 100,000 in 2008, and only 3000 in 1998 (Keller and Dance, September 2019). Again, these figures are just a fraction of the CSAM on the internet. In previous encryption battles, law enforcement warned of criminals and terrorists. In 2020, they have an emotionally and statistically more threatening enemy in child predators.

Where previous encryption battles threatened law enforcement's capacity to execute a warrant, E2EE threatens private companies' own surveillance of their platforms. As of today, many tech companies voluntarily search for CSAM via an algorithm called PhotoDNA. PhotoDNA is a simple algorithm; it first regularizes photos to remove minor differences in color, size and definition and then compares these photos to a database of CSAM. If a fingerprint of the regularized photo matches a database photo, then a NCMEC report is made (Keller and Dance, November 2019). Since in E2EE the server never sees the message, E2EE systems cannot run PhotoDNA and therefore cannot report CSAM to NCMEC.

In contrast with previous encryption battles, E2EE exists in a state of flux. IMessage, WhatsApp, and a few other apps use E2EE. Facebook Messenger, most messaging apps, and email do not use E2EE. While concerned with E2EE broadly, law enforcement is acutely concerned with preventing more platforms from adopting E2EE. Unfortunately for law enforcement, in March 2019 Facebook made the decision to use E2EE by default on all of their messaging apps. Zuckerberg noted the CSAM threat in his post: "Encryption is a powerful tool

for privacy, but that includes the privacy of people doing bad things … truly terrible things like child exploitation, terrorism, and extortion" (Zuckerberg, 2019). Bill Barr wrote a letter to Facebook asking them to hold off. He cites Facebook's own surveillance of CSAM: "This [E2EE] puts our citizens and societies at risk by severely eroding a company's ability to detect and respond to illegal content and activity, such as child sexual exploitation and abuse" (Patel et al. 2019). The Facebook E2EE initiative is especially critical because of how many reports Facebook generates. The Barr letter cites that Facebook generated 12 million of the 18.4 million CSAM reports last year. 99% of these reports are from the automated monitoring threatened by E2EE. Facebook generates so many reports because of how thoroughly they surveil their platforms for CSAM. Ironically, this hard work to fight CSAM puts the company under more pressure to maintain the status quo. Regardless, encryption opponents are able to cite a tangible loss in reports from Facebook's E2EE initiative.

E2EE opponents make a much-improved anti-encryption argument than before. Child predators are horrifying. CSAM is demonstrably massive. Furthermore, the solution they advocate for is not a meddling government. Rather, they ask private companies to maintain the status quo of non-E2EE systems. They cite a demonstrable loss if E2EE advances.

The Techlash

Facebook

In 2016, when Apple defied the FBI, pressure against large tech companies was only brewing. By 2020, that pressure has exploded. No company faced more pressure than Facebook. Rocked by the Cambridge Analytica data sharing scandal, manipulation of its platform by Russian trolls to influence the 2016 election, and various other security breaches and scandals,

the company's public relations are dreadful. In the eyes of the public, Facebook can do no good. With the importance of their CSAM reporting and their recent decision to encrypt all messaging services, Facebook is at the center of E2EE debate. The cynicism towards the company questions their motive in advancing E2EE. Critics write:

> Rather than meaningfully engage with Facebook's real issues, Zuckerberg invokes encryption to redirect the public from the difficult—and costly—reforms that would actually fix the social media platform. Call it "privacy laundering" (Rozenshtein, 2019).

Others wonder if Facebook's move toward E2EE is directed at CSAM and the like: "Once end-to-end encryption is put in place, Facebook can wash its hands of the content" (Tufekci, 2019). Facebook has been condemned for its various failings and the vilification has followed the company into the E2EE debate.

A good fight needs the right enemy. When fighting encryption was just about catching criminals, whom no one likes, the victim of encryption legislation was clearly individual privacy. In the Apple-FBI case, the debate broadened to include Apple's business model, but this played only a small role in this debate in part due to Apple's stellar reputation. In 2020, tech companies, and especially Facebook, provided an excellent foil to law enforcement in the encryption debate. Society is upset with how powerful and unaccountable these tech companies seem thus providing congress with a specific mandate to regulate.

Section 230

A focus point of the Techlash and the EARN IT Act is a law called Section 230. Part of the Communications Decency Act of 1996, Section 230 protects tech companies from what users do on their platforms. Without the protections, internet platforms as they exist today would be sued out of existence for what their users post. Section 230 lays out two protections known as the

shield and the stick. The shield protects platforms from being sued for what their users write. The stick gives platforms the right to moderate content without classifying them as curators responsible for the content. Recent criticism of Section 230 argues that tech companies have not used their stick sufficiently to moderate content (Molla and Stewart, 2019). Note that much of the Section 230 anger concerns public social networks where users post data for anyone to see. However, E2EE only works with private communications which have not been the subject of recent criticism.

In 2018, congress passed FOSTA (also SESTA), a bill that creates an exception to Section 230 with respect to sex workers. With FOSTA, Section 230 protections do not apply to civil and criminal charges of sex trafficking or conduct that promotes prostitution. As a result of this law, many websites shut down anything tangentially related to sex trafficking for fear of lawsuits. For example, Craigslist shut down its personals section for fear of misuse (Craigslist, 2018). This law has backfired in two ways: sex workers moved to more dangerous street work and law enforcement now complains of "blindness" to these crimes (Chamberlain, 2019). Despite these shortcomings, the law provides a blueprint for regulating tech companies by restricting Section 230 protections. The EARN IT Act follows this blueprint.

CSAM and E2EE are Difficult to Regulate

Before getting to the EARN IT Act, it is worth considering other approaches to CSAM and E2EE and why they are difficult. With CSAM, regulators must contend with 4th amendment issues with respect to companies' surveillance of their platforms. Meanwhile the 1st amendment is a concern when trying to regulate E2EE. Finally, technical approaches, such as backdoor proposals, remain fraught with social and technical issues.

4th Amendment and CSAM

Tech company surveillance of E2EE is spotty. The government could force tech companies to take stronger measures that would certainly catch more CSAM regardless of whether E2EE were allowed. However, the government must be careful. If the government forced companies to surveil their systems, tech companies would be acting as agents of government. Therefore under the 4th amendment, these surveillance and tip-line reports could not be used as evidence in court. The current law is careful to only require companies report CSAM that the companies become aware of (Reporting Requirements for Providers, 2008). The government is walking on thin ice with their push to have tech companies address CSAM (Pfefferkorn, March 2020). The current status quo is constitutionally valid, but other approaches may not be.

1st Amendment and E2EE

Outlawing E2EE directly is also fraught. Since Bernstein v. United States, encryption code is free speech, so a direct ban on the underlying cryptography would likely violate the first amendment. Compelling providers to insert encryption backdoors into products raises questions as well. For instance, in the FBI-Apple battle, Apple argued that compelling it to create a backdoor was compelled speech in violation of the 1st amendment. This argument went untested, so its validity is unclear. It is similarly unclear if the government could force providers to insert E2EE backdoors (Brumfield, 2019).

Backdoors Still Don't Work

In the 1990's the government tried to dictate technical requirements with the Clipper Chip. This failed miserably due to a flaw that made encryption possible as well as a lack of adoption of the chip in the marketplace (Blaze, 1994). In general, the government has struggled

to dictate technical requirements to tech companies. E2EE backdoors today are technically fraught as well.

A modern-day Clipper Chip, the Ghost Protocol, proposed by UK Law Enforcement officials, attempts to rewrite E2EE protocols to make warrants possible. The Ghost Protocol is an example of a key distribution attack. In a basic key distribution attack, Alice wants to send Bob a message so she gets his public key from the server. Except the server sends its own public key essentially turning the E2EE'd system into a non-E2EE'd system. In theory, the sender can and should check the key to confirm it belongs to the receiver and spot the attack; yet in practice, most users do not perform this check (Green, 2016). The Ghost Protocol works by secretly adding another public key belonging to law enforcement to the chat between Alice and Bob. Now, unknown to them, Alice and Bob's chat is a group chat with law enforcement (Levy and Robinson, 2018). 47 tech companies and nonprofits uniformly rejected this proposal on security and user trust concerns (Access Now et al. 2019).

The Earn It Act

The EARN IT Act works as follows. It would create a commission of 19 experts from industry and government headed by the Attorney General to generate recommendations for best practices related to CSAM. These best practices are ratified when 14 of the 19 experts agree on a set of best practices. Then, these recommendations are sent to the Attorney General, Secretary of Homeland Security, and FTC Chairman. If they approve, the best practices are sent to Congress for final approval. At this point, these best practices would create an exception to Section 230 with regards to CSAM. If providers follow the best practices, they are still protected from liability from users posting CSAM on their platforms. If they can prove in court they took

“reasonable measures” other than the best practices, they are protected as well. Otherwise, they lose protections against civil and state CSAM criminal cases (EARN IT, 2020). There are several issues with the EARN IT Act.

The EARN IT Act denies being about E2EE, but it is. Bill Barr, NCMEC, and law enforcement have all expressed disapproval of E2EE with regards to CSAM. E2EE is the obvious best practice the 19-member committee would look to eliminate. As former attorney advisor for the Department of Justice Alan Rozenshtein puts it: “I don't really see a realistic situation in which this does not implicate encryption” (Rodrigo, 2020). While E2EE is the elephant in the room, the bill never once mentions encryption. Cosponsor Senator Richard Blumenthal said “This bill is not about ending encryption,”(Rodrigo, 2020). The EARN IT Act seeks to avoid the difficult encryption debate by hiding its true intentions.

The EARN IT Act funnels Techlash anger with public platforms and Section 230 into private messaging. For example, critics argue Facebook did not do enough to prevent misinformation on the public Facebook app. This app is not private messaging. Section 230 may very well need to be changed; the debate over whether these companies use their stick enough is worth having. However, any regulation of Section 230 to address these concerns by focusing on the public platforms responsible for the concerns. Instead, the EARN IT Act is prepared to amend Section 230 to police private messaging services. Public platforms and private messaging are different. The EARN IT Act threatens to shift anger over public platforms into regulations on private messaging.

Section 230 exemptions are effectively law, without appearing so. Not following these best practices would be reckless. The legal threat of bearing even a fraction of responsibility for what users may do is just too high a risk for the tech companies. Unsurprisingly as FOSTA

showed, tech companies immediately shut down any potential source of liability. The EARN IT Act specifies that companies may retain protection if they take "reasonable measures". Even leaving this "reasonable measure" determination up to a judge would be too risky. As a result, these best practices would be treated as law despite only being "best practices". This capacity to write law indirectly is dangerous. These are difficult issues with hard constitutional and technical questions. They ought to be dealt with directly rather than via Section 230 exemptions.

Conclusion

The EARN IT Act is a deceptive bill. It threatens E2EE while avoiding debate as it avoids mentioning it. It conflates private messaging into public platforms leveraging Techlash anger into a separate domain. It governs indirectly by way of Section 230 exemptions rather than state law directly. As Riana Pfefferkorn of Stanford Law points out, the law that addresses the encryption of private messages over the internet is CALEA (Pfefferkorn, January 2020). Lawmakers could amend CALEA or write another law on E2EE or CSAM, but they should not pass the EARN IT Act.

CSAM is a horrible problem, so the government should give law enforcement more money to stop it. Big tech companies have abused their power and neglected their responsibility, so the government should regulate them. Unfortunately, opponents of E2EE have used these issues to malign E2EE. They risk tremendous privacy and security benefits in doing so.

References

Access Now, Big Brother Watch, Blueprint for Free Speech, Center for Democracy & Technology, Defending Rights and Dissent, Electronic Frontier Foundation, … Zimmerman, P. (2019, May 22). https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf

Barr, W. (2019, July 23). *International Conference on Cyber Security*. *International Conference on Cyber Security*. New York. https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber

Blaze, M. (1994). Protocol Failure in the Escrowed Encryption Standard. *AT&T Bell Laboratories*. https://www.mattblaze.org/papers/eesproto.pdf

Brumfield, C. (2019, November 4). US Department of Justice push for encryption backdoors might run afoul of First Amendment. https://www.csoonline.com/article/3450020/ us-department-of-justice-push-for-encryption-backdoors-might-run-afoul-of-first-amendment.html

Butz, A., & Schmitz, M. (2005). Design and applications of a beer mat for pub interaction. *Extended Proceedings of the Seventh International Conference on Ubiquitous Computing*. http://www.mmi.ifi.lmu.de/pubdb/publications/pub/butz2005ubicomp/butz2005ubicomp.pdf

Chamberlain, L. (2019). FOSTA: A Hostile Law with a Human Cost, 87 Fordham L. Rev. 2171 https://ir.lawnet.fordham.edu/flr/vol87/iss5/13

Clinton, B. (1998, January 27). C-SPAN. Immigration Policy and Counterterrorism. *1998 State of the Union Address*. https://www.c-span.org/video/?c4816430/user-clip-clinton-speeches-war-drugs-crime

Cook, T. (2016, February 24). ABC News. Interviewed by Muir, D. https://abcnews.go.com/Technology/exclusive-apple-ceo-tim-cook-iphone-cracking-software/story?id=37173343

Craigslist. (2018). about: FOSTA. https://www.craigslist.org/about/FOSTA

EARN IT Act of 2020, Senate. 116th Cong. (2020). https://www.judiciary.senate.gov/imo/media/doc/OLL20160.pdf

Freeh, L. (1995, March 30). *Excerpts from Congressional Testimony of Fbi Director Louis Freeh*. Before the House Committee on the Judiciary Subcommittee on Crime. https://www.epic.org/crypto/ban/freeh.html

Freeh, L. (1997, June 4). *Excerpts from Testimony by Louis Freeh*. Senate Judiciary Committee.

http://www.bugsweeps.com/info/freeh.html

Green, M. (2016, July 19). How do we build encryption backdoors? https://blog.cryptographyengineering.com/2015/04/16/how-do-we-build-encryption-backdors/

Hayden, M. (2015, December 18). C-SPAN. Immigration Policy and Counterterrorism. *Council on Foreign Relations*. https://www.c-span.org/video/?402284-1/discussion-immigration-policy-national-security

Keller, M. H., & Dance, G. J. (2019, September 29). The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong? https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html

Keller, M. H., & Dance, G. J. (2019, November 9). Child Abusers Run Rampant as Tech Companies Look the Other Way. https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html

Levy, I., & Robinson, C. (2018, November 29). Principles for a More Informed Exceptional Access Debate. https://www.lawfareblog.com/principles-more-informed-exceptional - access-debate.

Molla, R., & Stewart, E. (2019, December 5). Should social media companies be legally responsible for misinformation and hate speech? 2020 Democrats weigh in. https://www.vox.com/policy-and-politics/2019/12/3/20965459/tech-2020-candidate-policies-section230-facebook-misinformation-hate-speech

Patel, R. H. P. P., Barr, W. K., McAleenan, K., & Dutton, H. P. Open Letter: Facebook's "Privacy First" Proposals. (2019, October 4). https://www.justice.gov/opa/press-release/file/1207081/download

Pfefferkorn, R. (2020, January 30). The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning It. https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it

Pfefferkorn, R. (2020, March 10). The EARN IT Act Is Unconstitutional: Fourth Amendment. http://cyberlaw.stanford.edu/blog/2020/03/earn-it-act-unconstitutional-fourth-amendment

Reporting Requirements of Providers, Section 2258A. U.S. Code, Title 18. Crimes and Criminal Procedure. (2008). https://www.law.cornell.edu/uscode/text/18/2258A

Rodrigo, C. M. (2020, March 16). Bill to protect children online ensnared in encryption fight. https://thehill.com/policy/technology/487372-bill-to-protect-children-online-ensnared-in-encryption-fight

Rozenshtein, A. Z. (2019, October 31). Facebook, Encryption and the Dangers of Privacy Laundering. https://www.lawfareblog.com/facebook-encryption-and-dangers- privacy-laundering

Tufekci, Z. (2019, March 7). Zuckerberg's So-Called Shift Toward Privacy. https://www.nytimes.com/2019/03/07/opinion/zuckerberg-privacy-facebook.html

Vance, C. (2016, February 21). NPR Interviewed by Martin, R.https://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock

Zuckerberg, M. (2019, March 6). A Privacy-Focused Vision for Social Networking. https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/