The US Government, Encryption, and the Perennial Crypto Wars

Shreyas Minocha

From its origins in government research labs, modern encryption has come a long way. Not only does it allow governments and companies to protect their secrets, but it also allows individuals to browse and communicate free from the fear of being snooped on, facilitating freedom of expression and privacy. Over the past few decades, however, the US government has been trying to control and restrict access to encryption, citing—primarily—concerns around counter-terrorism, criminal investigations, and exploitation of children. This paper explores the history of such attempts, focusing on their motivation, scope, and impact. We shall find that they share similar flaws, including a lack of transparency, neglect of the civil liberties afforded by encryption, and a disregard for the opinions of security experts.

Introduction

The practice of using ciphers to protect secrets has been around for hundreds of years. While for the longest time access to secure means of encryption was limited to governments and intelligence agencies, starting in the 1960s and 70s, these tools started to become increasingly widespread and increasingly accessible. The publishing of the Data Encryption Standard (DES) in the 1970s and the invention of public-key cryptography in the mid-70s would serve as catalysts for the advancement and proliferation of modern cryptography. Companies and businesses would also come to adopt encryption to protect their secrets from corporate espionage. Over the next few

decades, as communications and data storage would grow increasingly go digital, encryption would find itself in the hands of individuals, either through tools offered by technology companies or through open-source software like Pretty Good Privacy (PGP).

In the present day, where the internet is the means for a bulk of our communication, encryption protects the right of individuals to be able to express themselves anonymously and free of fear of persecution. From protecting victims of stalking to helping protestors around the world safely organize, there's no question that encryption has tangible benefits to democratic society.[1] For instance, organizers of the Freddie Gray protests used encrypted texting apps to avoid being harassed by law enforcement.[2] Activists frequently use encrypted tools in response to frequent warrantless monitoring of legal activism, in the US and especially so in regions with more repressive governments. Journalists, too, use end-to-end encrypted apps like Signal to communicate with informants, who might risk their jobs, freedom, or even their lives in the absence of encryption.[3] Encryption protects the very people responsible for holding governments accountable. Additionally, we presently live in a "golden age of

---

[1] Riana Pfefferkorn, "A Response to 'Responsible Encryption'," 2017, https://cyberlaw.stanford.edu/blog/2017/10/response-%E2%80%9Cresponsible-encryption%E2%80%9D.

[2] Brandon E. Patterson, "'Black People Need Encryption,' No Matter What Happens in the Apple-FBI Feud," 2016, https://www.motherjones.com/politics/2016/03/black-lives-matter-apple-fbi-encryption/.

[3] Matthieu Aikins, "The Spy Who Came in from the Code," 2012, https://archives.cjr.org/feature/the_spy_who_came_in_from_the_c.php.

surveillance"[4], where the privacy of our communications and identities is under more threat than ever. Encryption enables us to have a sphere of privacy in the digital world, and thus goes hand-in-hand with the right to privacy.

Unfortunately, the encryption technology that empowers the average individual also grants the same powers to malicious actors. However, the fact that some abuse their rights for evil is seldom reason enough to strip millions of those rights. In the late 1980s, the NSA began to fear the impact of widespread encryption on their intelligence-gathering mission. This would spark off a decades-long saga—often referred to as the "Crypto Wars"—of attempts at chipping away at the freedoms afforded by these tools, for the sake of law enforcement's convenience. These attempts have taken a variety of forms but they share similar rhetoric. They frequently allude to the false dichotomy between "warrant-proof encryption", and supporting and enabling criminals. This view doesn't consider the fact that this technology offers people means to exercise their right to privacy, and by extension, other rights enshrined in the constitution. As such, these attempts are consistently met with backlash from civic liberty groups, most journalists, and often even the public at large. They are frequently short-sighted, and designed without enough consultation with cryptography experts and thus fail to account for nuances unique and inherent to the nature of cryptography. In this paper, we shall look

[4] Peter Swire and Kenesa Ahmad, "Encryption and Globalization," 2011, https://doi.org/10.2139/ssrn.1960602.

at some examples of the government's attempts to cripple modern encryption (hence "strong encryption" or just "encryption"), examine their flaws, and look for these trends in their implementation, scope, and response.

Infiltrating Standards

Dual_EC_DRBG

The generation of random numbers is at the heart of encryption. One important quality of a "good" random generator is that it is not deterministic: the numbers generated by it at any instant cannot be used to predict the numbers it will generate in the future. In 2017, the National Institute of Standards and Technology (NIST) published a paper that included four recommended algorithms for random number generation. One of these, *Dual_EC_DRBG*, stood out from the rest. Developed at the NSA, Dual EC would soon gain notoriety in the cryptography community and raise concerns surrounding the NSA's involvement in the standards process, considering its dual motivations: "[providing] the United States [...] the best possible codes" and "cracking ciphers and providing great intelligence"[5].

It was in 2006—even before the algorithm was published in the NIST standard—that security researchers first pointed out flaws in Dual EC, disproving a weakly supported

[5] Steven Levy, *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age* (Viking Penguin, 2001).

claim about the generator's security made by the NIST paper. In a 2007 presentation, cryptographers with Microsoft Research pointed out an even more concerning flaw in the algorithm which, according to security researcher Bruce Schneier, "can only be described as a backdoor".[6] The presentation takes issue with a certain unexplained constant Q in the algorithm and shows that if someone—say the algorithm designer—knew the constant d associated with the generation of Q, they could trivially predict future outputs of the generator.[7] Whether anyone knows the constant d and whether this flaw was introduced deliberately is subject to speculation. In any case, this has ruinous implications for the algorithm's suitability for cryptography applications. Applications using the algorithm would be vulnerable to exploitation by someone who knows, or comes to know the constant d.

Schneier expressed confusion regarding the inclusion of the flawed algorithm in the NIST publication, remarking "It makes no sense as a trap door: It's public, and rather obvious. It makes no sense from an engineering perspective: It's too slow for anyone to willingly use it".[8] However, use it people did. In 2013, Reuters reported that RSA Security, a network security company, received $10 Million from the NSA to set Dual

---

[6] Bruce Schneier, "Did NSA Put a Secret Backdoor in New Encryption Standard?" 2007, https://www.wired.com/2007/11/securitymatters-1115/.

[7] Dan Shumow and Niels Ferguson, "On the Possibility of a Back Door in the NIST Sp800-90 Dual Ec Prng," 2007, http://rump2007.cr.yp.to/15-shumow.pdf.

[8] Schneier, "Did NSA Put a Secret Backdoor in New Encryption Standard?".

EC as the default algorithm for their BSafe software.[9] RSA denied designing or enabling any backdoors, while the NSA declined to comment. It was only in 2013, years after Dual EC's flaws were discovered, that RSA advised its customers against using the algorithm. In 2014, NIST too withdrew its recommendation. If the NSA did deliberately push for the publication of a flawed, backdoored standard, as there is reason to believe, it would be an unfortunate sign of the NSA's ability to covertly and recklessly compromise the world's security infrastructure. This threatens not just the security of the communications of American companies and individuals, but also their constitutional rights, all without any form of oversight. The allegations of paying RSA Security to use the vulnerable standard are even more frightening, highlighting the lengths to which the NSA will go to further its intelligence-gathering mission.

The Snowden revelations in 2013 led to a resurgence in discussion about the role of the NSA at large, but also about their role in the drafting and publishing of Dual EC. In 2015, Michael Wertheimer, a retired NSA official, published an article titled 'The Mathematics Community and the NSA', following the publication of several articles about the matter in the Notices of the AMS, most of them critical of the NSA. In the article, he calls the NSA's continued endorsement of the standard "regrettable". However, he also spends a large part of the article defending Dual EC, pointing out, for

[9] Joseph Menn, "Exclusive: Secret Contract Tied NSA and Security Industry Pioneer," 2013, https://web.archive.org/web/20131221000408/http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.

instance, that it was just one of four algorithms in the standard. For this reason, and because the letter merely addresses the continued endorsement of Dual EC and not its introduction, it was viewed by some as a "non-apology" that only deepened the divide between the agency and the cryptography community.[10] Following these controversies, the NIST announced changes to their cryptographic standards development process to regain the trust of stakeholders, including cryptographic experts. This new process would allow for a more rigorous process of review and public input. While these changes —which were endorsed by Wertheimer in his letter—are a commendable initiative, a thorough accounting of the circumstances surrounding the publication of Dual EC would've been the responsible thing for the agency to do; it would have also done more to repair the public's trust in the agency's involvement in the cryptographic standards process.[11]

[10] Dan Goodin, "NSA Official: Support of Backdoored Dual_EC_DRBG Was 'Regrettable'," 2015, https://arstechnica.com/information-technology/2015/01/nsa-official-support-of-backdoored-dual_ec_drbg-was-regrettable/; Matthew Green, "Hopefully the Last Post i'll Ever Write on Dual EC DRBG," 2015, https://blog.cryptographyengineering.com/2015/01/14/hopefully-last-post-ill-ever-write-on/.

[11] Green, "Hopefully the Last Post i'll Ever Write on Dual EC DRBG.".

Influencing Providers

Clipper Chip

In the late 1980s and early 1990s, some NSA officials raised the alarm about a problem that they'd term "going dark": the fear that as encryption increasingly became available to the public, the agency would lose its ability to gather intelligence. Their solution was the Clipper Chip, "a device meant to encrypt communications, but with a built-in backdoor" ("key escrow"). A device with the chip would be assigned a secret key; two "escrow agents"—later announced to be the NIST and a division of the Treasury Department—would be given half a key each. When the government "established authority" to decrypt a communication, the escrow agents would hand over the keys for that communication. The agency hoped that the chip would be adopted by providers, which would allow them to intercept the communications of their customers. However, the chip was met with widespread criticism and neither consumers nor providers embraced it. By 1996, it was all but defunct. While this attempt at subverting encryption didn't come to fruition, it is an important part of the history of encryption in the United States and the first chapter in the Crypto Wars.

The encryption mechanism used by the Clipper chip, Skipjack, was also developed by the NSA. Until June 1998, long after the Clipper chip was abandoned, the algorithm was classified as SECRET, which made public scrutiny impossible. Given the

importance of peer review in the cryptography community, this lack of transparency was one of the reasons for backlash against the chip. Clinton Brooks, the creator of the Clipper chip, had hoped to do things differently. In a meeting with NSA officials, Brooks made a case for having the NSA collaborate with the public. He foresaw the importance of gaining the trust of the industry and the public at large. His ideas were quickly shot down, however: the approach was too much of a departure from the NSA's typical *modus operandi*.[12] This fits in with the NSA's pattern of obscuring the details of their cryptographic endeavours, instead of being transparent and forthcoming. An issue like cryptography, with its implications ranging from industrial competitiveness to individual freedom, wasn't just going to go under the radar as the government had hoped. Regardless of whether Skipjack itself was cryptographically sound, the NSA's decision to shroud it in secrecy was an irresponsible move, and it did little to gain the favour of the public.

Several logistical considerations regarding the export of the Clipper chip weren't taken seriously in the rush to develop and deploy it. While the chip would be free of the strict export restrictions that typically applied to encryption at the time, it was unclear why foreign governments would want their citizens to use tools that only the US government had backdoored access to. Would the US allow foreign governments access to communications of their citizens? Even governments notorious for human rights abuses

[12] Levy, *Crypto*.

and stifling of free speech? No one knew; while these concerns were brought up before Clipper was announced, little was done to address them in an example of the government pushing under-specified, poorly thought-out solutions to the supposed encryption problem.[13] Additionally, it was unlikely that foreign companies would want security systems that the US government held the keys to. After all, they could just buy tools equipped with strong encryption elsewhere. Moreover, the tech industry was afraid that backdoored encryption would hurt American economic competitiveness.[14]

Conventional wisdom in the cybersecurity world advises "The human is the weakest link". The fact that key escrow systems—including Clipper—rely on humans to control and limit access to keys leaves them particularly vulnerable to insider abuse. The motivations for this sort of abuse can be varied, including greed, extortion, and recklessness.[15] With Clipper, insider abuse by employees at the escrow agents could compromise communications of individuals, corporate secrets, and even national secrets. Similarly, the key recovery databases and the identities of the key recovery agents would be valuable targets for attackers looking to compromise communications. By impersonating law enforcement agents, for instance, an attacker could gain access to the

---

[13] Levy.

[14] John Markoff, "Flaw Discovered in Federal Plan for Wiretapping" (The New York Times, 1994), https://www.nytimes.com/1994/06/02/us/flaw-discovered-in-federal-plan-for-wiretapping.html.

[15] Hal Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 1997.

mechanisms to decrypt communications. These weaknesses are further magnified at scale, as are the costs associated with developing and maintaining such systems.[16]

The largest current of backlash, however, was not about the technical or logistical limitations of the Clipper chip. People saw a system where the government held the keys to everyone's communications regardless of their innocence or guilt as Orwellian and un-American. John Perry Barlow of the Electronic Freedom Frontier, for instance, felt that the Clipper chip would eventually lead to the end of freedom in America.[17] In his testimony to the Congress in 1993, Whitfield Diffie, one of the pioneers of public-key cryptography, urged his audience to recognize the right to private conversation and warned of a world where "privacy will only belong to the rich".[18] Computer Professionals for Social Responsibility, an organization promoting responsible use of technology, collected over 50,000 signatures on a petition calling the Clinton administration to withdraw Clipper.[19] The Clipper debate was everywhere, and an overwhelming majority of people sided against the government on the issue.[20]

---

[16] Abelson et al.

[17] Levy, *Crypto*.

[18] Whitfield Diffie, "The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology," 1993, https://archive.epic.org/crypto/clipper/diffie_testimony.html.

[19] Steven Levy, "Battle of the Clipper Chip" (The New York Times, 1994), https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.

[20] Levy, *Crypto*.

In 1994, Bell Labs scientist Mathew Blaze would discover a vulnerability in the Clipper chip's key escrow system that would doom its prospects of success. This flaw and others would highlight that escrow systems—by virtue of having substantially more complex requirements—are much harder to get right than strong encryption, which is hard enough as it is.[21] While these issues have been demonstrated time and again, they seem to fall on deaf ears. Perhaps the officials that authorize these initiatives don't understand the technical and logistical complexities tied with backdoored encryption and aren't willing to learn from the experts. Blaze had discovered a way to trick Clipper into sending messages with the purportedly secure Skipjack algorithm, but with invalid metadata which would make it impossible for law enforcement to retrieve the keys that were used in the communications. This particular flaw was a result of the rush to design and deploy Clipper. NSA engineers had hoped to design the chip in a way that would make Blaze's exploit less practical, but in another example of the government ignoring experts, the FBI insisted on prioritizing the ease with which they could decrypt communications instead.[22]

Eventually, the combination of its technical vulnerabilities and the backlash from security experts, industry, and civilians contributed to Clipper's lack of adoption. By 1996, the Department of Justice was the only significant purchaser of the chip; the

---

[21] Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption.".

[22] Levy, *Crypto*.

Clipper chip was practically irrelevant. Notably, the chip was swiftly approved by the White House in spite of its many flaws. If it weren't for its technical vulnerabilities and the work of the organizations that fervently argued against its adoption, Clipper may well have been successful in gaining a critical mass of adoption. Many of the trends we saw in the Clipper chip case would feature time and again in subsequent iterations of the Crypto Wars.

San Bernardino attack

In December 2015, Syed Rizwan Farook and his wife Tafsheen Malik carried out a mass shooting in San Bernardino, California, killing 14 and injuring 22. While the perpetrators died in a shootout with police later that day, Farook's employer-issued iPhone 5C was retrieved. Unable to access the password-protected data on the phone, the Justice Department directed Apple to provide "reasonable technical assistance to assist law enforcement in obtaining access to the data". In particular, this would involve Apple creating a custom version of iOS with several security features disabled—a backdoor to let the bureau into the phone. This request was made under the All Writs Act of 1789, which since 2008, has been regularly used by the FBI to compel tech companies to unlock electronic devices. When faced with this order, however, Apple issued a statement opposing the order. Since the order would have implications well beyond this particular case, this led to public discourse about encryption as it relates to

privacy and law enforcement. In March 2016, the FBI withdrew its request, having successfully broken into the phone with the aid of a third party.

In its 2016 letter to its customers, Apple explains its reasons for opposing the order. While expressing remorse over the events of the shooting and a willingness to cooperate with the FBI by, say complying with valid subpoenas, they argue that the FBI's request was unprecedented, a threat to its consumers, and a dangerous precedent.[23] Indeed, a backdoor—like the one requested by the FBI—would impact the security of all Apple customers, including millions of law-abiding citizens. Tools like the one requested by the FBI are dangerous in the hands of adversaries—eavesdroppers, corporate spies, or adversarial foreign governments. Regardless of procedural safeguards put in place to limit access to them, backdoors are vulnerabilities waiting to be exploited.

An important facet of Apple's argument against the FBI's order was that their compliance would set a "dangerous precedent". The application of the aforementioned All Writs Act to compel providers to write backdoored software would be a broad expansion of the government's power to reach into people's devices. A precedent of successful use of the All Writs Act for something of this sort could then be abused to compel Apple to write more dangerous backdoors, Apple argues. Governments around the world, including highly repressive and authoritarian regimes, would also pressure

[23] Tim Cook, "A Message to Our Customers" (Apple Inc., 2016), https://www.apple.com/customer-letter/.

Apple into hacking into their citizens' devices.[24] Once software to backdoor devices exists and a precedent of its use is established, it's tough to put the genie back into the bottle.[25] After all, there is no lack of examples of tech companies acquiescing to unreasonable demands of governments around the world, from Yahoo's cooperation with the Chinese government in the early 2000s to Twitter's standoff with the Indian government as recently as 2021. It is telling that the FBI tried to practically repurpose a 200-year-old statute to apply to the unlocking of electronic devices. If they were successful in establishing such a precedent, the FBI would effectively bypass the checks and balances such as the Congress that are meant to keep the government accountable. This is not unlike the many instances of the government repurposing the Computer Fraud and Abuse Act to prosecute data scraping (as in *United States v. Swartz*), improper access of computer files (as in *Van Buren v. United States*), and more. This practice of shoe-horning new issues into old laws is unfortunately particularly common with laws as applied to digital technology. There's no substitute for writing new laws as technology and its role in society evolves. The same goes for laws about encryption.

The assertion that Apple's assistance was strictly necessary for the government to access the data on the phone was an important part of the government's order—the All Writs

---

[24] Amar Toor, "EFF, ACLU, and Amnesty International Voice Support for Apple in FBI Battle," 2016, https://www.theverge.com/2016/2/18/11044642/apple-fbi-encryption-eff-aclu-amnesty-snowden.

[25] Pfefferkorn, "A Response to 'Responsible Encryption'.".

Act requires "[t]he absence of alternative remedies". However, Daniel Kahn Gillmor, Senior Staff Technologist at the ACLU voiced suspicions that the FBI deliberately mischaracterized the necessity of Apple's cooperation in their order. As Gilmor explains, the auto-erase function that the FBI wishes to bypass works not by erasing all the files on the phone, but by erasing the key that the files were encrypted with, effectively rendering the files inaccessible. This key is stored on the flash storage of the phone, but by using widely available tools, the FBI could just create a copy of that part of the phone's storage. This would give them as many attempts as they may need to break into the phone using the "enormous computing power in the US government" and "without the phone killing itself".[26] It is unlikely that the FBI's experts weren't already aware of this, which raises the question of what the FBI's intentions with these legal pursuits were. As we shall see, they were likely an attempted power grab.

In March 2016, the government revealed that it managed to access the data on Farooq's phone and withdrew the order requesting Apple for assistance.[27] Since the order was reliant on the fact that the contents of the phone could not be accessed "by any other means known to either the government or Apple", it was no longer enforcible. While the FBI revealed little about how they managed to bypass the device's security features,

[26] Daniel Kahn Gillmor, "One of the FBI's Major Claims in the iPhone Case Is Fraudulent" (ACLU, 2016), https://www.aclu.org/blog/privacy-technology/internet-privacy/one-fbis-major-claims-iphone-case-fraudulent.

[27] USA v. In the matter of the search of an apple iPhone seized during the execution of a search warrant on a black lexus IS300, california license plate 35KGD203 (2016).

"it's unlikely to grant the broad powers that the proposed GovtOS would have"[28]. With this attempt at broadening the scope of its decryption powers unsuccessful, the government would turn to other means. Notably, Melanie Newman, spokesperson for the Justice Department, said in a statement:

> "It remains a priority for the government to ensure that law enforcement can obtain crucial digital information to protect national security and public safety, either with cooperation from relevant parties, or through the court system when cooperation fails [...] We will continue to pursue all available options for this mission [...]"

Contrary to FBI Director James Comey's claims that the FBI-Apple standoff "[wasn't] about trying to set a precedent", this comment clearly suggests that it was, indeed, more than about just one phone. It was a strategy to further the government's perennial goal of breaking encryption, which in this case capitalized on the fear resulting from the horrific San Bernardino shooting. In the words of Daniel Gillmor, it was a "power grab": an attempt to add to its toolset, by way of establishing legal precedent, this dangerous ability. Since 2016, the government has, indeed, continued to attempt to reduce access to—and even outlaw—strong encryption; there are no signs that they will stop.

---

[28] Russell Brandom, "Apple's San Bernardino Fight Is Officially over as Government Confirms Working Attack," 2016, https://www.theverge.com/2016/3/28/11317396/apple-fbi-encryption-vacate-iphone-order-san-bernardino.

Apple was commended for its stance against the government's attempts to establish these dangerous precedents. However, in a healthy democracy, Apple wouldn't have even found itself in such a predicament. In Edward Snowden's words, "The [FBI] is creating a world where citizens rely on [Apple] to defend their rights, rather than the other way around". Indeed, the government should engage with the concerns raised by citizens, researchers, and organizations and take action to protect encryption, and by extension fundamental rights. Unfortunately, far from defending the right to encryption, the US government has shown time and again that it will go to any length to contain and cripple encryption in the hands of its citizens.

Introducing Encryption Legislation

US EARN IT Act

Sponsored by Senators Lindsey Graham and Richard Blumenthal, the EARN IT Act 2020 was introduced ostensibly to combat online sexual exploitation of children; the bill would limit the scope of Section 230 of the Communications and Decency Act, which protects platforms from liability against user-generated content and is largely responsible for freedom of expression on the internet. The bill proposed the formation of a national commission to develop a set of "best practice guidelines" for providers of interactive computer services. Providers would then be required to adhere to these

guidelines, lest they lose their section 230 immunity: they'd have to "earn" the immunity. While the bill didn't directly address encryption, it would've allowed the commission members to prevent providers from implementing end-to-end encryption[29]—a right they're entitled to under other laws—and was widely condemned as a "sneak attack on encryption".

The bill came amid heightened concerns around the online sexual exploitation of children. Indeed, Child Sexual Abuse Material (CSAM) on the internet has been growing at an alarming rate.[30] However, EARN IT was by no means not the first attempt at controlling CSAM. 18 U.S. Code § 2258A requires providers to take several steps to limit online sexual exploitation of children. When they become aware of sexual exploitation of children on their platforms, providers must file a report to the CyberTipline system of the NCMEC. As long as providers follow these steps upon learning of violations, they are protected from liability for third-party content.[31] Indeed, there's evidence that tech companies are complying with Federal CSAM law, reporting

[29] Riana Pfefferkorn, "The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning It," 2020, https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it.

[30] Michael H. Keller and Gabriel J. X. Dance, "The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?" 2019, https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

[31] "Reporting Requirements of Providers, u.s. Code 18 § 2258a," n.d.

over 45 million illegal photos and videos in 2018 alone.[32] If they weren't reporting child abuse content they found on their platforms, the government would have grounds to sue them under CSAM law. Yet—according to a government press release—the EARN IT bill was drafted because, given the (limited) immunity afforded by Section 230 of the Communications Decency Act, "many companies do not aggressively go after online child sexual exploitation".[33] If so, the straightforward solution would've been to propose amendments to CSAM law, and increase what the law requires of these companies. By instead threatening the limited immunities offered by section 230, lawmakers were dressing up yet another attack on encryption in the guise of a law to protect children from online sexual exploitation.

While some senators, such as Blumenthal, claimed that the bill was not about encryption, then-Attorney General William Barr had on multiple occasions made his intent to crack down on encryption clear.[34] For instance, in a July 2019 speech at the International Conference on Cybersecurity, he remarked "we must ensure that we retain

---

[32] Michael H. Keller and Gabriel J. X. Dance, "The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?" 2019, https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

[33] "Graham, Blumenthal, Hawley, Feinstein Introduce EARN IT Act to Encourage Tech Industry to Take Online Child Sexual Exploitation Seriously" (Committee on the Judiciary, 2020), https://www.judiciary.senate.gov/press/rep/releases/graham-blumenthal-hawley-feinstein-introduce-earn-it-act-to-encourage-tech-industry-to-take-online-child-sexual-exploitation-seriously.

[34] Joe Mullin, "The EARN IT Bill Is the Government's Plan to Scan Every Message Online" (Electronic Frontier Foundation, 2020), https://www.eff.org/deeplinks/2020/03/earn-it-bill-governments-not-so-secret-plan-scan-every-message-online.

society's ability to gain lawful access to data and communications when needed to respond to criminal activity". The commission appointed following the EARN IT bill, if it were passed, would vest in the same Attorney General veto power over the guidelines. In what policy experts described as a "bait-and-switch" [35], the government reframed its not-so-subtle attempt at cracking down on encryption in terms of Section 230. This framing took benefit of a wave of criticism of "big tech" companies at the time. Additionally, it used the admirable goal of protecting children from sexual exploitation as yet another vehicle to further law enforcement's misguided goal of undermining strong encryption.

The indirection with which EARN IT attacked encryption was particularly insidious. Under the Communications Assistance for Law Enforcement Act (CALEA) of 1994, providers have the right to implement end-to-end-encryption in their products. Rather than proposing amendments to CALEA and engaging in a public conversation about encryption and law enforcement, the bill sidestepped the issue, instead potentially slipping it in by means of the "best practice guidelines" commission. This would make providers that implement end-to-end encryption liable for merely exercising their rights under CALEA. It's likely that this was a tactic to avoid the inevitable backlash that would come with directly threatening encryption. The FBI has been trying to get rid of

[35] Pfefferkorn, "The EARN IT Act.".

the end-to-end encryption provisions of CALEA for years, but with little success.[36] EARN IT was thus a trojan horse, seeking to covertly achieve this dangerous goal.

The issues with EARN IT don't end there. In addition to threatening encryption, it was also unlikely to significantly control the distribution of CSAM. If good-faith platforms complied with the best practice guidelines, nothing would stop CSAM traders from simply moving to other, bad-faith platforms including those dedicated to the sharing of such content. There, they would be even harder to track down. Additionally, some of these platforms don't even qualify for immunity under section 230, since they either have a role in the production of the illegal content they host, or they just ignore their 2258A duties. Since they operate illegally as-is, the threat of losing immunity is moot. As a result, the innocent majority on good-faith platforms would suffer, losing access to strong encryption, with little to make up for it. Additionally, offenders that stay on good-faith platforms could always just encrypt their files before sending them using widely available encryption software.[37] After all, criminals keep up with law enforcement techniques and are increasingly competent in protecting themselves using state-of-the-art technology.[38]

---

[36] Pfefferkorn, "The EARN IT Act.".

[37] Pfefferkorn.

[38] Keller and Dance, "The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?".

Following backlash, the bill underwent some amendments that prohibited holding companies liable for using encryption. However, the bill still threatened encryption: it encouraged state lawmakers to look for ways to undermine end-to-end encryption, a move reminiscent of the fate of net neutrality under the Trump administration. With its covert threats to encryption, contradictions with CALEA, and practical flaws with respect to actually limiting distribution of CSAM, EARN IT serves as an example of how not to write laws that deal with digital issues, especially encryption.

Conclusion

In this paper, we looked at some examples of the US government's attempts at dealing with—or rather, controlling—strong encryption. While the specific techniques used to attempt to cripple encryption have evolved, the government's attitude towards encryption has been consistently flawed since the 1990s.

One theme common throughout the Crypto Wars has been the government's secrecy and lack of transparency. When the Clipper chip was introduced, the workings of the encryption algorithm it used—Skipperjack—were kept hidden from the public, classified SECRET. This was particularly unwelcome in the cryptography community where "security by obscurity" is frowned upon. In the words of Bruce Schneier, "The U.S.

government is on a secrecy binge".[39] This extends beyond attempts at thwarting encryption, encompassing the NSA's widespread domestic surveillance, the FBI's interception of cell phone data, and more. Unfortunately, what we do know of these activities isn't because the government is forthcoming about it. Transparency and accountability are crucial to the democratic project, and this rings true especially for an issue like encryption, which is—by every measure—a human rights issue.[40] Encryption is unique in that public standards and protocols are often safer than those that are shrouded in secrecy. Formal and informal processes of review in the security and math communities play an important role in this. It's thus important that government officials work with these communities and value their input.

Since the ill-fated Clipper chip, some of the government's attempts at undermining encryption have employed greater degrees of indirection. This ties back in with the severe lack of transparency. For instance, in *Apple v. FBI*, the government sought to expand their powers to compel providers to undermine the security of their products by way of establishing legal precedent. Indeed, *Apple v. FBI* was not about a single phone used by a terrorist, or even by terrorists in general: it would hurt everyone's privacy. Yet, officials claimed otherwise. With the EARN IT bill, this was taken a step further:

---

[39] Bruce Schneier, "What We Don't Know about Spying on Citizens: Scarier Than What We Know" (The Atlantic, 2013), https://www.theatlantic.com/politics/archive/2013/06/what-we-dont-know-about-spying-on-citizens-scarier-than-what-we-know/276607/.

[40] Wolfgang Schulz and Joris van Hoboken, "Human Rights and Encryption," 2016.

the bill didn't even mention encryption, but would all but outlaw it. The government line, in some cases, was to dismiss accusations of the law targeting encryption altogether. This is dangerous and antithetical to the tenets of democracy; transparency and open, honest dialogue in Congress about the issues at stake in the encryption debate is the need of the hour.

Perhaps most consistent, and most damning, of the flaws of the government's approach to encryption is their ignorance or indifference towards the many legitimate uses of encryption. Sure, government officials do their token acknowledgement of the merits of encryption in protecting government secrets, in industrial applications, and occasionally in defending the rights and freedoms of civilians. However, little serious consideration is given to the privacy and civil liberty ramifications of the proposals and moves to compromise encryption. The right of citizens to have means of communication free of surveillance is seldom considered in these bargains. When the government was preparing to announce the Clipper chip, it did not anticipate the degree to which backlash, along civil liberty lines, would be targeted at the move.[41] In the commission that the EARN IT act hoped to establish, no representatives would be appointed to speak for users of civil society.[42] This goes to show the government's consistent disregard for this important aspect of encryption use.

---

[41] Levy, *Crypto*.

[42] Pfefferkorn, "The EARN IT Act.".

A healthier approach towards encryption would involve recognizing the importance of strong encryption—to industry and to civilians—and steering clear of attempts to threaten it. Instead, working with security experts on ways to satisfy legitimate law enforcement needs without compromising or outlawing encryption would be more productive. Meanwhile, we must not let fear—of terrorists, child abusers, or otherwise—be used to justify sweeping abuses of human rights via erosion of encryption.