ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

# Why New Calls to Subvert Commercial Encryption Are Unjustified

DANIEL CASTRO | JULY 2020

Law enforcement argues that "warrant-proof" encryption presents a unique and urgent threat by preventing them from accessing user data. But history shows that government efforts to subvert encryption would negatively impact individuals and businesses. As such, banning the technology is not the answer.

## KEY TAKEAWAYS

- Encryption gives individuals and organizations the means to protect the confidentiality of their data, but it has interfered with law enforcement's ability to prevent and investigate crimes and foreign threats.
- Technological advances have long frustrated some in the law enforcement community, giving rise to multiple efforts to subvert commercial use of encryption, from the Clipper Chip in the 1990s to the San Bernardino case two decades later.
- Having failed in these prior attempts to circumvent encryption, some law enforcement officials are now calling on Congress to invoke a "nuclear option": legislation banning "warrant-proof" encryption.
- This represents an extreme and unjustified measure that would do little to take encryption out of the hands of bad actors, but it would make commercial products less secure for ordinary consumers and businesses and damage U.S. competitiveness.

## INTRODUCTION

Law enforcement has a long history of surreptitiously intercepting messages to prevent and investigate crimes and foreign threats. However, the steady development, adoption, and use of encryption—the process of transforming information to disguise its meaning—has interfered with that capability by giving individuals and organizations the means to protect the confidentiality of their data. These technological changes have frustrated some members of the law enforcement community, giving rise to multiple high-profile efforts to subvert commercial use of encryption, from the Clipper Chip in the 1990s to the San Bernardino case more than 20 years later.

**Banning "warrant-proof encryption" represents an extreme and unjustified "nuclear option" that would do little to take encryption out of the hands of bad actors, but would make commercial products used by ordinary consumers and businesses less secure and damage U.S. competitiveness.**

Some law enforcement officials now argue that they face a unique and urgent threat from "warrant-proof encryption"—encryption where only the users, and not any third-party, hold the keys to access the data. In particular, law enforcement is frustrated by efforts by the tech industry to reduce security risks by implementing end-to-end encryption on messaging apps and encrypting data on mobile devices. However, a close look at the key events that have shaped law enforcement access to encrypted data reveals that the ability of law enforcement to successfully access user data has varied at different points in history due to technological and legal limits.[1] Moreover, calls by law enforcement for Congress to pass legislation banning "warrant-proof encryption" represent an extreme and unjustified measure—a "nuclear option"—that would do little to take encryption out of the hands of bad actors, but would make commercial products used by ordinary consumers and businesses less secure and damage U.S. competitiveness.

## A BRIEF HISTORY OF THE ENCRYPTION DEBATE

Early methods used to encrypt information have evolved over time, from the basic substitution ciphers used by Julius Caesar to more advanced polyalphabetic substitution ciphers invented by Thomas Jefferson and Charles Babbage. While encryption has long been used to protect the confidentiality of written communications, its importance increased with the rise of electronic communications networks—including telegraph and telephone networks and radio broadcasts—which can more easily be intercepted. For example, the Confederate Army used the Vigenère cipher, created in 1553 and thought to be unbreakable for hundreds of years, to protect sensitive military communications sent via telegraph during the U.S. Civil War, and the Germans used the Enigma machine to encrypt radio transmissions during World War II.[2] Militaries tightly controlled access to their most advanced ciphers to protect the confidentiality of their communications and gain an advantage over their adversaries.

As civilian use of electronic communications networks increased, law enforcement began using wiretaps for criminal investigations. For example, in the 1920s, federal agents used wiretaps of telephones to investigate bootlegging cases during Prohibition.[3] The U.S. Supreme Court initially ruled in *Olmstead v. United States* that there were no Constitutional protections limiting law enforcement from using wiretaps, but after Congress passed the Federal Communications Act in 1934, the Court later reversed course and established limits on when government could conduct electronic surveillance without a warrant. Eventually, Congress formalized this authority when it passed the Omnibus Crime Control and Safe Streets Act of 1968, permitting the use of wiretaps for a limited number of serious crimes, such as murder, kidnapping, and extortion.[4] Congress expanded law enforcement authority again in 1978 with the Foreign Intelligence Surveillance Act (FISA), which legalized wiretaps for national security purposes. In 1986, Congress passed the Stored Communications Act, as part of the Electronic Communications Privacy Act, which established conditions for when law enforcement could lawfully compel access to customer data held by third parties.

Up until the mid-1970s, most public methods of encryption were more art than science. However, this changed with the development of modern encryption protocols based on rigorous mathematical techniques to assure the confidentiality of information.[5] These advances included the development of standardized, publicly available symmetric key encryption protocols (algorithms that use the same key to both encrypt and decrypt data), such as the Data Encryption Standard (DES) in 1977, and public-key encryption protocols such as RSA in 1978. (The National Institute of Standards and Technology eventually replaced the DES algorithm with the Advanced Encryption Standard [AES] in 2001 after activists showed that the algorithm could be successfully cracked using relatively inexpensive hardware.[6])

The development of public key encryption was particularly important given the parallel advancements in wide area networking, such as the creation of ARPAnet, the precursor to the Internet. The challenge with symmetric key algorithms is that, alone, they are poorly suited for sharing information securely among multiple parties because all parties must share a secret key. Securely distributing keys is a non-trivial problem, often requiring the use of a trusted courier or an in-person meeting, and impractical in many situations. In contrast, public key encryption uses two keys, one public and one private.[7] The public key can be shared openly, and it is used to encrypt messages that only the private key can decrypt. Advances in public key encryption enabled the development of the Secure Sockets Layer (SSL), a cryptographic protocol designed by Netscape in 1994 to let clients and servers communicate securely over the Internet.[8] Importantly, SSL enabled Internet users to complete secure transactions online, such as online shopping and banking.[9]

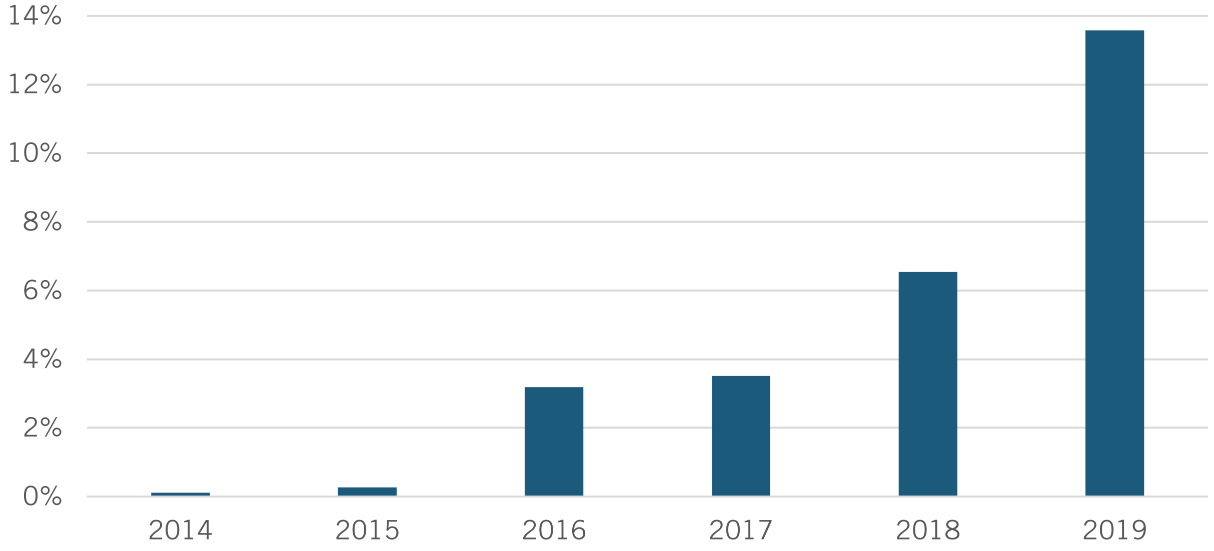
The 1990s saw growing tensions between government efforts to control encryption and commercial and academic interest in the field. Concerns about privacy and government intrusion led to the development of Pretty Good Privacy (PGP), an open-source public-key encryption program created by Phil Zimmermann in 1991, to enable anyone to sign and encrypt files and messages. Originally created to secure files stored on bulletin board systems, PGP quickly found an audience online as the Internet blossomed.[10] After Zimmerman published his software, the U.S. government investigated him for violating export controls (PGP used a minimum of 128-bit keys, enabling significantly stronger encryption than was allowed to be exported at the time), but eventually dropped its case.[11] While Zimmerman's dispute with the U.S. government attracted a lot of attention, the main fight in what would be later referred to as the "Crypto Wars" came later.[12]

**Figure 1: Timeline of key events in the debate over encryption**

| Year | Key Events |
|---|---|
| 1553 | Vigenère cipher created |
| 1837 | Telegraph invented |
| 1863 | Vigenère cipher broken |
| 1876 | Telephone invented |
| 1895 | Radio transmission invented |
| 1928 | U.S. Supreme Court ruled that wiretaps for telephone conversations are not protected by the Fourth or Fifth Amendments in *Olmstead v. United States* |
| 1934 | U.S. Federal Communications Act passed prohibiting "interception and divulgence" of wired communications |
| 1968 | Omnibus Crime Control and Safe Streets Act passed legalizing wiretaps for criminal investigations |
| 1969 | ARPAnet launched first packet-switched wide area network |
| 1976 | Diffie-Hellman key exchange created |
| 1977 | Apple II, Commodore PET 2001, and TRS-80 released |
| 1977 | Data Encryption Standard (DES) created |
| 1978 | RSA public-key cryptosystem published |
| 1978 | Foreign Intelligence Surveillance Act (FISA) passed legalizing wiretaps for national security purposes |
| 1985 | First dot-com domain name registered on the Internet |
| 1986 | Stored Communications Act (SCA) passed establishing conditions for law enforcement access to customer data |
| 1990 | First website on the World Wide Web published |
| 1991 | PGP ("Pretty Good Privacy"), an open source encryption algorithm, distributed online |
| 1993 | Clipper Chip developed |
| 1994 | Clipper Chip vulnerabilities published |
| 1994 | Communications Assistance for Law Enforcement Act (CALEA) passed requiring digital telephone networks to be built with wiretap capabilities |
| 1994 | Secure Sockets Layer (SSL) released |
| 1998 | DES cracker built for less than $250,000 |
| 2001 | Advanced Encryption Standard (AES) created |
| 2013 | Snowden documents leaked revealing global surveillance of commercial systems |
| 2014 | Apple and Google announced mobile operating systems will encrypt users' data by default |
| 2016 | FBI demanded access to encrypted iPhone used in San Bernardino terrorist attack |
| 2016 | WhatsApp enabled end-to-end encryption |
| 2019 | UK, US, and Australian law enforcement officials requested Facebook not implement end-to-end encryption on its messaging service |
| 2020 | FBI demanded access to encrypted iPhones owned by Pensacola Naval Air Station shooter |

The FBI's Advanced Telephony Unit warned in 1992 that if a key escrow system was not created, by 1995, at least 40 percent of wiretaps would be useless—an estimate that, as figure 2 shows, greatly overestimated the problem.[13] In response, the U.S. National Security Agency (NSA) developed a tamper-resistant hardware encryption module, known as the Clipper chip, in 1993, which it proposed companies use to encrypt telephone and data communications. However, a key function of the Clipper chip was that it would implement a key escrow system to enable law enforcement to easily decrypt any encrypted information.[14] Under the initial scheme, the U.S. Department of Treasury's Automated Systems Division and NIST would hold escrowed keys.[15] There was strong public opposition to the plan, especially among digital activists, academics, and technology companies, and after Matt Blaze, a computer scientist at AT&T's Bell Laboratories, found a critical vulnerability, the government eventually dropped the proposal.[16]

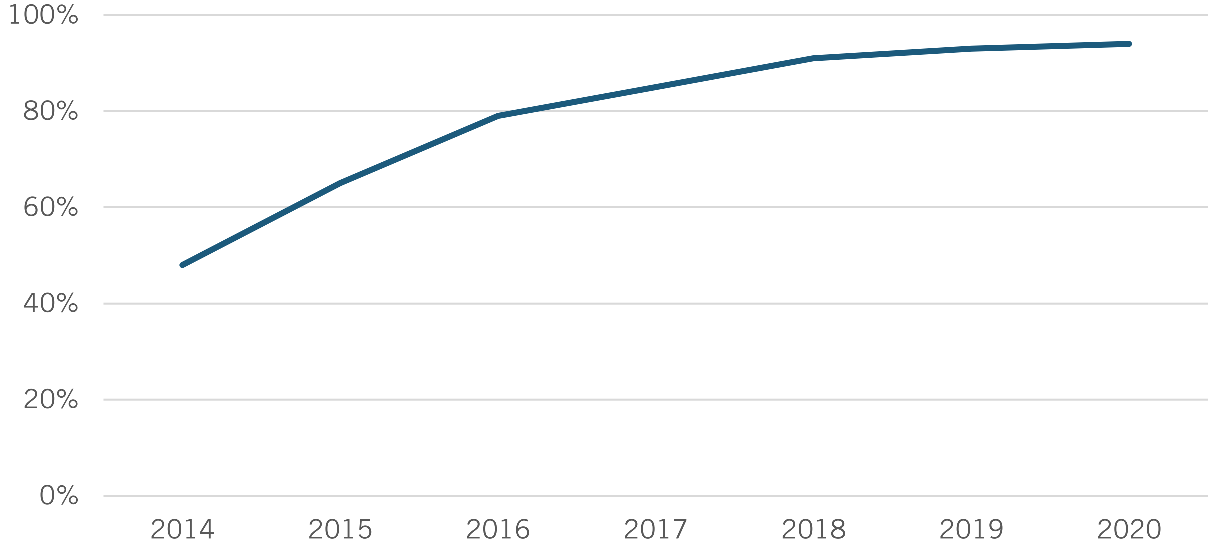
**Figure 2: Percent of state and federal wiretaps law enforcement were unable to access because of encryption, 2014–2019***



*Source: Administrative Office of the U.S. Courts*[17]

The debate over encryption received little attention in subsequent years until NSA contractor Edward Snowden leaked documents in 2013 showing that the NSA and other intelligence agencies were collecting user information directly from popular online services.[18] In response to mounting public concern about privacy, many companies expedited initiatives to increase security, such as by enabling encryption by default in mobile operating systems, enabling full-disk encryption on personal computers, and enabling end-to-end encryption in online messaging services. For example, as shown in figure 3, the percent of encrypted traffic across Google products and services has nearly doubled since 2014.

**Figure 3: Percent of encrypted traffic across Google, 2014–2020**



*Source: Google*[19]

Law enforcement officials have grown increasingly concerned at the loss of access to user data that these advancements in encryption have brought about. In 2014, James Comey, then director of the FBI, stated, "The law hasn't kept pace with technology, and this disconnect has created a significant public safety problem."[20] The issue became front-page news in 2016 when the FBI obtained a writ from a U.S. magistrate ordering Apple to make software that would allow the government to access the contents of an encrypted iPhone found in possession of one of the deceased terrorists after an attack in San Bernardino, California.[21] Apple refused and the dispute headed to court, but six weeks later the FBI backed down because a forensic company it had hired successfully accessed the data on the phone. However, the law enforcement community continued to complain about the impact of encryption on its investigations, with FBI Director Christopher Wray repeatedly claiming that encryption prevented investigators from gaining access to nearly 7,800 devices during fiscal year 2017.[22] The FBI later admitted this statistic was significantly inflated, stalling momentum for those calling for change.[23]

U.S. Attorney General William Barr reignited the debate in July 2019 when he claimed in a high-profile speech that "by enabling dangerous criminals to cloak their communications and activities behind an essentially impenetrable digital shield, the deployment of warrant-proof encryption is already imposing huge costs on society."[24] That same month, an alliance of U.S. national intelligence partners, including Australia, Canada, New Zealand, and the United Kingdom, jointly called for government access to encrypted communications.[25] Then in October 2019, the U.S. Department of Justice hosted a high-profile conference linking end-to-end encryption with child exploitation, and sent an open letter to Facebook, signed by counterparts from the UK and Australia, requesting that the company halt its plans to implement end-to-end encryption on its messaging service because this would hurt child safety.[26]

In December 2019, the U.S. Senate Judiciary Committee held a hearing on encryption where the committee Chairman Senator Lindsey Graham told representatives of Apple and Facebook that if they did not provide law enforcement access to encrypted communications, members of Congress would introduce legislation requiring them to do so.[27] In the subsequent months, the U.S. Department of Justice continued to apply public pressure on tech companies, lambasting them in public remarks for designing their systems so that only users could access their encrypted data and calling for legislation to enable law enforcement to gain access.[28] Senator Graham, true to his word, introduced the Lawful Access to Encrypted Data Act in June 2020, which would require tech companies to provide a means for law enforcement to access encrypted data when ordered by a judge, effectively barring them from using end-to-end encryption.[29] Attorney General Barr endorsed the legislation, arguing that "end-to-end encryption technology is being abused by child predators, terrorists, drug traffickers, and even hackers to perpetrate their crimes and avoid detection."[30]

This history shows that law enforcement access to consumer data has varied over time as the technology and law has changed. It is true that for several years encryption did not interfere with law enforcement's ability to obtain access to user data stored by a third party, such as email stored in the cloud. But government has not always had unfettered access to encrypted user data. Law enforcement never had a direct means by which to decrypt data when the user held the key; rather, it was limited to using brute force methods. For example, in the 1980s and 1990s, law enforcement had no practical way to access data users encrypted with DES since no third party had access to the keys. (Intelligence services, on the other hand, could likely use brute force to break the encryption, although that process was still expensive and inefficient.) And users in the 1990s could use PGP to protect their emails and files, even if relatively few chose to do so.

But the argument that "warrant-proof" encryption creates a novel problem misrepresents the reality of law enforcement: Search warrants give law enforcement officials the right to search a location for specific items; it does not guarantee them the ability to find what they are looking for. For example, search warrants will not produce evidence that is sufficiently well-hidden or information that is memorized but never written down. Encrypted data is not a new problem, it is an old one.

## GOVERNMENT EFFORTS TO SUBVERT COMMERCIAL USE OF ENCRYPTION

Over the years, the U.S. government has used numerous methods to subvert commercial use of encryption, including limiting academic research, imposing export controls, promoting key escrow, introducing secret backdoors, exploiting vulnerabilities, and compelling software or hardware changes. These efforts are misguided because they put all users—indeed the same users law enforcement aims to protect—at greater security risk.

### Limiting Academic Research

The U.S. government has sought to limit researchers from publicly disclosing information about encryption.[31] For example, at one point, the NSA attempted to take control of funding for encryption research from the National Science Foundation.[32] When these efforts failed, the NSA began using the 1951 Invention Secrecy Act to classify encryption research by non-government actors as secret, preventing researchers from sharing their findings publicly.[33] For example, in 1977, when Professor George Davida of the University of Wisconsin and freelance researcher Carl Nicolai filed separate patents for encryption products, the NSA sent both an order declaring their work classified and prohibiting them from sharing it.[34] The two researchers ultimately refused to comply and published their work, generating enough publicity and support from the academic community that the NSA decided to rescind the gag orders. The courts have also upheld the right of academics to conduct and publish this type of research.[35]

## Imposing Export Controls

Since World War II, the U.S. government has strictly controlled the export of encryption for national security reasons.[36] Indeed, it was not until 1996 that President Bill Clinton issued an executive order that reclassified encryption as being a "dual-use technology" rather than "munitions" that were illegal to export.[37] As a result, the U.S. approach to export controls on encryption has often deviated from that of other nations. For example, the Coordinating Committee for Multilateral Export Controls (COCOM), an international organization of 17 member countries, recommended in 1991 to allow export of mass-market encryption software and public domain software.[38] Although the United States was a member of COCOM, it did not follow its recommendations. COCOM was dissolved in 1994, and in 1996, the United States led a group of 33 nations to adopt the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Originally the Wassenaar Arrangement mirrored COCOM's rules, but in 1998, members revised the Wassenaar Arrangement to only allow export of mass-market encryption software with a maximum key length of 64 bits. However, many countries disregarded this policy. For example, for many years, the United States did not allow companies to export encryption with a key size greater than 56 bits, even after signing on to the Wassenaar Arrangement.[39] In contrast, European nations that signed on to the Wassenaar Arrangement continued to liberalize their encryption export policies. Moreover, there are several countries that export encryption products and are not a party to the Wassenaar Arrangement. As a result, U.S. export controls on encryption have had a limited effect.

## Promoting Key Escrow

The government has encouraged the use of key escrow systems to enable extraordinary access to encrypted information. In 1991, Congress passed legislation that included non-binding language calling for hardware makers to provide a mechanism by which law enforcement could gain access to the decrypted contents of voice, data, and other communications when lawfully authorized.[40] As noted previously, in 1993, the NSA also developed and began promoting the Clipper Chip, a computer chip that implemented an NSA-backed algorithm to encrypt telephone and data communications using a key escrow system.[41] After security researchers publicly disclosed vulnerabilities in the Clipper Chip, the U.S. government backed away for this particular implementation but continued to push for the private sector to implement its own key escrow systems.[42]

## Introducing Secret Backdoors

The government has secretly introduced backdoors in encryption standards. For example, NSA manipulated a public encryption standard used to produce random numbers and paid a security company to make this standard its default.[43] The impact of these types of backdoors can be substantial. For example, in 2015, Juniper Networks, a tech company that makes networking equipment, discovered that this vulnerability led to adversaries being able to decrypt encrypted network traffic in some of its products.[44]

## Exploiting Vulnerabilities

The government can also exploit vulnerabilities to gain access to protected data. For example, in 2019 WhatsApp disclosed that an Israeli company that sells its services to governments around the world had exploited a vulnerability in its software to install spyware on the devices of its users to surveil them.[45] While encryption algorithms may be highly secure, exploiting vulnerabilities in related systems or stealing passwords—i.e., hacking into these devices—allows the government to circumvent encryption.[46]

### Compelling Software or Hardware Changes to Facilitate Government Hacking

Law enforcement has tried to compel companies to make changes to their systems to facilitate government hacking of encrypted data. As noted earlier, the FBI attempted to use the All Writs Act to demand Apple create custom software that would circumvent the security on the iPhone and allow federal investigators use a brute force attack—trying all possible password combinations until they find the correct one—to access encrypted data on a suspect's phone.[47]

## NEW CALLS FOR A BAN ON "WARRANT-PROOF ENCRYPTION"

While the law enforcement and intelligence communities have made various attempts to subvert commercial use of encryption in the Internet era, until recently, these efforts have fallen short of the most extreme tactic—the nuclear option—that policymakers could pursue: a legislative ban on commercial use of certain types of encryption.

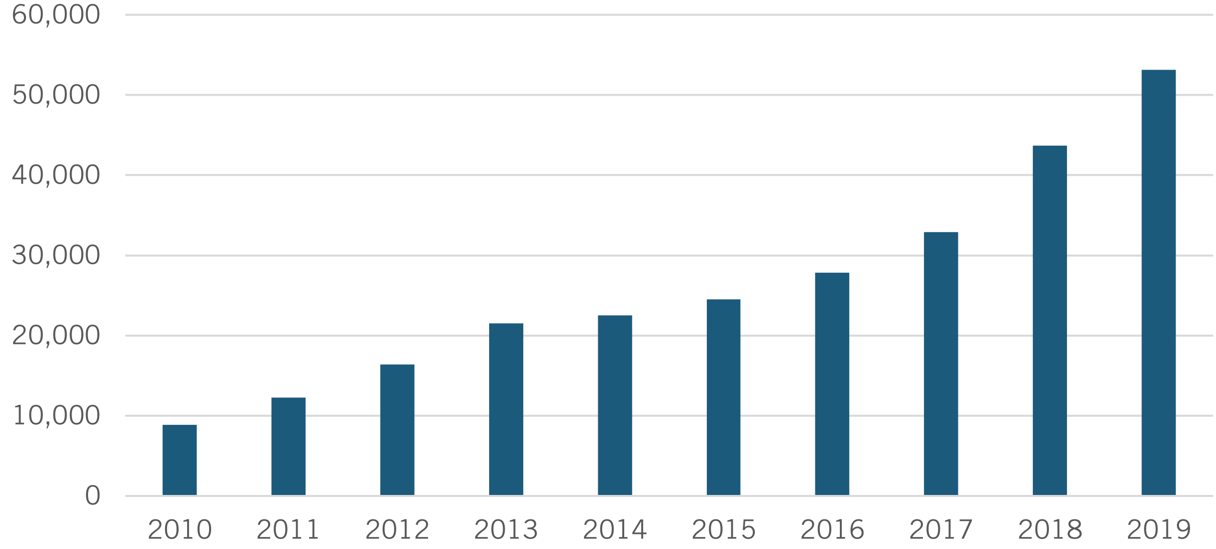
There are many reasons law enforcement has not previously pursued this option. First, despite repeated attempts by law enforcement to blame encryption for interfering with investigations into terrorist attacks, there is still not strong public support to undermine encryption to strengthen law enforcement. For example, polls found that more Americans sided with Apple over the government when the company refused to cooperate with the FBI's request to create custom software to allow it to bypass the security of the phones used by the San Bernardino shooters.[48]

Second, despite the public complaints leveled against tech companies by law enforcement, virtually every major Internet platform routinely cooperates with law enforcement behind the scenes to lawfully gather evidence, detect and remove illegal content, and address many different types of online crime.[49] So while some law enforcement officials would prefer that these companies do not offer products where users control access to the encrypted data, they recognize that these companies are still valuable law enforcement partners.

Third, even when law enforcement is unable to directly gain access to encrypted user data, they can still gain access to valuable metadata, including location data from mobile devices, call records, and email headers. Metadata is not encrypted, and companies provide government this information when they receive a lawful request.[50] While the volume of encrypted user data is certainly increasing, the amount of metadata available to law enforcement is also growing. As shown in figure 4, law enforcement has seized this opportunity, and the number of U.S. government requests for user information from Google has increased nearly six-fold in the past decade.

But this detente has come to an end. The U.S. Department of Justice now argues that failure to provide law enforcement exceptional access to encrypted data would be disastrous, and that there is an urgent need for reform. As noted, these arguments have been made many times before. In the 1990s, this was the justification for the Clipper Chip and export controls on encryption.

**Figure 4: Number of U.S. government requests for user information from Google, 2010–2019**



*Source: Google*[51]

So why is law enforcement now pursuing a legislative option? For one, they see their window of opportunity rapidly closing. As more online service providers implement end-to-end encryption and hardware makers encrypt the contents of their devices by default, consumers will increasingly expect these features and resist efforts by government to make the products less secure.

Second, Congress has generally held a favorable view of the tech sector, recognizing its contributions to the economy and society, and as a result, has been reluctant to pursue policies that could hurt the industry. But a growing "techlash" over the past few years, where critics have blamed tech companies for a variety of social and economic problems, has weakened the industry's political capital.[52] This has created an opportunity for a variety of the tech industry's critics, including law enforcement, to promote their own legislative agendas.

Third, law enforcement has become more strategic in its messaging to the public and Congress. Much of the past debate on encryption focused on its impact on law enforcement broadly, especially the ability to investigate or prevent terrorism domestically. However, law enforcement has shifted that message over the past year to focus on the impact of encryption on law enforcement's ability to investigate child sexual abuse material. For example, Attorney General Barr stated, "Survivors of child sexual abuse and their families have pleaded with technology companies to do more to prevent predators from exploiting their platforms to harm children. We cannot allow these companies to elevate their profits and the privacy rights of these abusers over the safety and security of children."[53] This tactic is likely a result of law enforcement recognizing the successful playbook used to pass a controversial set of bills—the Fight Online Sex Trafficking Act (FOSTA) in the House, and the Senate's Stop Enabling Sex Traffickers Act (SESTA)—where advocates of the law were able to overcome strong tech industry opposition by arguing that they were acting in the interests of child sex trafficking victims.[54]

Finally, U.S. law enforcement has seen some other countries move forward with legislation limiting encryption. The United Kingdom has sought to limit end-to-end encryption by passing the Investigatory Powers Act, dubbed the Snoopers Charter, in 2016.[55] This law could force companies to alter their use of end-to-end encryption so that they can fulfill the requirement that they provide requested customer data upon request. In May 2019, GCHQ, a UK intelligence agency, also proposed that companies "silently add a law enforcement participant to a group chat or call" to enable them to access these communications.[56] Similarly, in 2018, the Australian parliament passed legislation that requires companies to provide law enforcement and intelligence agencies with access to encrypted data.[57] Companies that refuse to comply with the law face fines of up to A$10 million ($7 Million).

## THE IMPACT OF SUBVERTING ENCRYPTION

Law enforcement argues that the benefits of limiting encryption would be substantial and the costs minimal. But they are overstating the benefits and understating the costs. Indeed, there are two problems with this argument.

First, efforts to limit or subvert commercial encryption in the United States would ultimately do little to keep the technology out of the hands of terrorists or criminals who want it. If bad actors want to use encryption, they can easily find tools to do so from open-source software or foreign providers. Encryption methods are now in the public domain, thus anyone with the technical proficiency can build these tools on their own. Indeed, in 2007, al-Qaeda developed software, known as Mujahideen Secrets, to encrypt their online communications.[58] Similarly, immediately following the 2013 Snowden leaks about U.S. surveillance, three terrorist organizations—GIMF, the Al-Fajr Technical Committee, and ISIL—each created a new encryption tool.[59] Moreover, when bad actors use foreign tools, domestic law enforcement and security agencies also lose access to metadata from U.S. providers. Certainly, some bad actors might continue to use less secure technologies, especially in the short term before alternatives become more widely adopted, so this would make it easier for law enforcement to gain access to some information. However, limiting commercial encryption in the United States would not eliminate the main concern raised by law enforcement because bad actors would still be able to encrypt data and keep it out of the hands of law enforcement.

Second, the costs of subverting commercial encryption would be substantial because they undermine the competitiveness of U.S. businesses and reduce privacy and security for ordinary individuals and businesses.

It is important to remember that the United States does not have a monopoly on encryption technology. A 2016 survey of 865 hardware and software products incorporating encryption from fifty-five countries found that two-thirds of these products come from non-U.S. providers and that several of the smaller foreign firms stored source code in multiple countries, making it easy for them to relocate if a country passes a law limiting encryption.[60] Some of the most advanced work in encryption comes from outside the United States — the current NIST-approved standard for encryption, AES, was developed by two Belgian cryptographers.[61]

Third, subverting encryption would negatively impact global trust in U.S. technology companies. Past U.S. export restrictions on encryption enabled foreign companies—such as F-secure in Finland and Aladdin in Israel—to gain significant market advantage throughout the world at the expense of U.S. companies.[62] More recently, several U.S. companies have described how the Snowden leaks damaged their ability to do business abroad.[63] And after Australia adopted its law limiting encryption, the Australian Department of Home Affairs wrote a report acknowledging that the law has had a "material impact on the Australian market and the ability of Australian companies to compete globally" in the communications and technology industry.[64]

Finally, the biggest impact of limiting encryption would fall on law-abiding individuals and businesses. It is important to understand that any kind of back door (or front door) access for the "good guys" can also be exploited by the "bad guys." For example, key escrow systems would introduce new attack vectors that could allow attackers to gain access to encrypted information, such as by compromising the system that maintains copies of the keys. Indeed, past efforts to weaken encryption standards or not disclose known vulnerabilities to allow government to circumvent encryption have negatively impacted the security of all users, including government users who often use the same technology as the private sector.[65]

## CONCLUSION

Given long-standing opposition to restrictions on commercial encryption from civil society, academics, and technology companies, the debate over encryption will remain a hotly contested policy issue for the near future. Moreover, the steady deployment of ever-more-secure technologies will mean that encryption will continue to impact the methods and operations of law enforcement and the intelligence community, and these communities will have to adapt to new circumstances. There is room for reasonable debate about how to respond to this challenge and how to better equip law enforcement with the tools and resources it needs to make use of digital evidence.[66] But the U.S. government's policy should be to champion encryption at home and abroad as a foundation for a more secure and trustworthy Internet. As such, legislative proposals to ban "warrant-proof encryption" or otherwise provide law enforcement with exceptional access to encrypted data—the nuclear option—should be off the table as they would ultimately be ineffective and shortsighted, sacrificing long-term gains in cybersecurity and national competitiveness for short-term law enforcement capabilities.

## Acknowledgments

The author wishes to thank Ashley Johnson for collecting data, and Alan McQuinn and Rob Atkinson for providing input to this report. Any errors or omissions are the author's alone.

## About the Author

Daniel Castro is the vice president of ITIF and the director of ITIF's Center for Data Innovation. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

## About ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

## ENDNOTES

1. "Going Dark," Federal Bureau of Investigation, n.d. https://www.fbi.gov/services/operational-technology/going-dark.
2. "A new cipher code," (Scientific American Supplement, January 27, 1917), 83 (2143): 61.
3. Susan Landau, "Security, Wiretapping, and the Internet," *IEEE Security and Privacy*, 2005, 26:33.
4. Ibid.
5. Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography, second edition.* (Chapman & HallCRC Press, 2014).
6. "Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197," NIST, November 26, 2001, https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf, and "Cryptographic Standards and Guidelines," NIST, December 29, 2016, https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects`/aes-development.
7. Niels Ferguson and Bruce Schneir, *Practical Cryptography* (Wiley Publishing, 2003).
8. Rolf Oppliger, *SSL and TLS: Theory and Practice, Second Edition* (Artech House, 2016).
9. Ibid.
10. Philip Zimmerman, "Why I Wrote PGP," *PhilZimmermann.com,* 1991, updated in 1999, https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.
11. Bernstein v. United States Department of Justice, No. 97-16686, (9th Cir. May 6, 1999), http://caselaw.findlaw.com/us-9th-circuit/1317290.html.
12. Steven Levy, *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*, (Penguin Books, 2001).

[13] Federal Bureau of Investigation Advanced Telephony Unit, “Telecommunications Overview 1992,” *Columbia University*, January 4, 2016, https://www.cs.columbia.edu/~smb/Telecommunications_Overview_1992.pdf.

[14] Brittany Bieber et al., “Civil Liberties Vs National Security in the Encryption Debate: Exceptional Access and the Trust Deficit,” *Cyber Security: A Peer-Reviewed Journal*, Vol. 2, No. 4, Summer 2019, 360-386, https://www.ingentaconnect.com/content/hsp/jcs/2019/00000002/00000004/art00008.

[15] Ibid.

[16] Matt Blaze, “Key Escrow from a Safe Distance: Looking Back At the Clipper Chip,” (ACSAC, 2011) https://www.mattblaze.org/papers/escrow-acsac11.pdf.

[17] Wiretap Reports, 2014-2019, Administrative Office of the U.S. Courts, n.d. https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports (accessed July 9, 2020).

[18] Timothy Lee, “Here’s everything we know about PRISM to date,” *Washington Post*, June 12, 2013, https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

[19] “HTTPS encryption on the web,” Google Transparency Report, n.d. https://transparencyreport.google.com/https/overview?hl=en (accessed July 9, 2020).

[20] James Comey, “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” *Federal Bureau of Investigation*, October 16, 2014, accessed July 16, 2019, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[21] Ian Williams, “The Secrets We Keep…: Encryption and the Struggle for Software Vulnerability Disclosure Reform,” 25 Mich. Telecomm. & Tech. L. Rev. 105 (2018), https://repository.law.umich.edu/mttlr/vol25/iss1/4.

[22] Christopher Wray, “Raising Our Game: Cyber Security in an Age of Digital Transformation” Federal Bureau of Investigation, Fordham University, January 9, 2018, accessed May 15, 2019, https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation.

[23] “FBI repeatedly overstated encryption threat figures to Congress, public,” *Washington Post*, May 22, 2018, https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html.

[24] William Barr, “Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security,” U.S. Department of Justice, July 23, 2019, accessed July 24, 2019, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

[25] “Joint Meeting of FCM and Quintet of Attorneys-General” Five Country Ministerial, 2019, accessed July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822120/Joint_Meeting_of_FCM_and_Quintet_of_Attorneys_FINAL.pdf.

[26] “Attorney General Barr Signs Letter to Facebook From US, UK, and Australian Leaders Regarding Use of End-To-End Encryption,” U.S. Department of Justice, October 3, 2019, https://www.justice.gov/opa/pr/attorney-general-barr-signs-letter-facebook-us-uk-and-australian-leaders-regarding-use-end.

[27] Sen. Graham stated, “You're gonna find a way to do this or we're gonna do it for you. We're not going to live in a world where a bunch of child abusers have a safe haven to practice their craft.” “Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy,” Committee on the Judiciary, U.S. Senate, December 10, 2019, https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy.

28. “Attorney General William P. Barr Announces Updates to the Findings of the Investigation into the December 2019 Shooting at Pensacola Naval Air Station,” U.S. Department of Justice, May 18, 2020, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-updates-findings-investigation-december-2019.

29. “Graham, Cotton, Blackburn Introduce Balanced Solution to Bolster National Security, End Use of Warrant-Proof Encryption that Shields Criminal Activity,” U.S. Senate Committee on the Judiciary, June 23, 2020,, https://www.judiciary.senate.gov/press/rep/releases/graham-cotton-blackburn-introduce-balanced-solution-to-bolster-national-security-end-use-of-warrant-proof-encryption-that-shields-criminal-activity.

30. “Statement from Attorney General William P. Barr on Introduction of Lawful Access Bill in Senate,” U.S. Department of Justice, June 23, 2020, https://www.justice.gov/opa/pr/statement-attorney-general-william-p-barr-introduction-lawful-access-bill-senate.

31. Susan Landau et al., Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy, Association for Computing Machinery Inc., New York, June 1994, pp. 37-38, https://www.acm.org/binaries/content/assets/public-policy/1994_usacm_report_crypto.pdf.

32. In 1977, the NSA approached Fred Weingarten, the director of the National Science Foundation, arguing that federal law gave the intelligence agency control over cryptography funding. Weingarten disputed these claims. David Banisar, “Stopping Science: The Case of Cryptography” Health Matrix 253, Vol. 9, Iss. 2, 1999, https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1483&context=healthmatrix.

33. Ibid.

34. Charles Sykes, *The End of Privacy* (New York: St. Martin’s Press, 1999), 173.

35. Bernstein v. United States Department of Justice, No. 97-16686, (9th Cir. May 6, 1999), http://caselaw.findlaw.com/us-9th-circuit/1317290.html; Junger v. Daley, No.98-4045, (6th Cir. 2000), http://caselaw.findlaw.com/us-6th-circuit/1074126.html.

36. U.S. Congress, Office of Technology Assessment, Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information, OTA-CIT-31O (Washington, DC: U.S. Government Printing Office, October 1987).

37. “Executive Order 13026 of November 15, 1996, Administration of Export Controls on Encryption Products,” Federal Register, Vol. 61, No. 224, November 19, 1996, https://www.govinfo.gov/content/pkg/FR-1996-11-19/pdf/96-29692.pdf.

38. Karim K. Shehadeh, “The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests.” American University International Law Review 15, no. 1 (1999): 271-319.

39. “Executive Order 13026 of November 15, 1996, Administration of Export Controls on Encryption Products,” Federal Register, Vol. 61, No. 224, November 19, 1996, https://www.govinfo.gov/content/pkg/FR-1996-11-19/pdf/96-29692.pdf.

40. Comprehensive Counter-Terrorism Act of 1991, S. 266, 102nd Cong. (1991), https://www.congress.gov/bill/102nd-congress/senate-bill/266/text.

41. Brittany Bieber et al., “Civil Liberties Vs National Security in the Encryption Debate: Exceptional Access and the Trust Deficit,” Cyber Security: A Peer-Reviewed Journal, Vol. 2, No. 4, Summer 2019, 360-386, https://www.ingentaconnect.com/content/hsp/jcs/2019/00000002/00000004/art00008.

42. Matt Blaze, “Protocol Failure in the Escrow Encryption Standard,” *AT&T Bell Laboratories*, August 20, 1994, http://www.cryptomuseum.com/crypto/usa/files/eesproto.pdf.

43. Larry Greenemeier, “NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard,” *Scientific American*, September 18, 2013, https://www.scientificamerican.com/article/nsa-nist-encryption-scandal/ and Joseph Menn, “Exclusive:

NSA infiltrated RSA security more deeply than thought,” *Reuters*, March 31, 2014, https://www.reuters.com/article/us-usa-security-nsa-rsa/exclusive-nsa-infiltrated-rsa-security-more-deeply-than-thought-study-idUSBREA2U0TY20140331.

44. ”Where Did I Leave My Keys?: Lessons from the Juniper Dual EC Incident,” Communications of the ACM, Vol. 61, Iss. 11, November 2018, accessed July 23, 2019, 148-155, https://dl.acm.org/citation.cfm?id=3266291.

45. *WhatsApp Inc. v NSO Group*, “Complaint, Demand for a Jury Trial,” October 29, 2019, https://www.washingtonpost.com/context/read-the-whatsapp-complaint-against-nso-group/abc0fb24-8090-447f-8493-1e05b2fc1156/.

46. Chen-Yu Li et. al., “A Comprehensive Overview of Government Hacking Worldwide” IEEE Access, Vol. 6, 2169-3536, September 2018, accessed July 23, 2019, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8470931.

47. Ibid.

48. “Solid support for Apple in iPhone encryption fight,” Reuters, February 24, 2016, https://www.reuters.com/article/us-apple-encryption-poll-idUSKCN0VX159.

49. “Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance,” Developments in the Law – More Data, More Problems, Harvard Law Review, 2018, https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/

50. “Don’t Panic: Making Progress on the ‘Going Dark’ Debate,” Berkman Center for Internet & Society at Harvard University, February 1, 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

51. “Global requests for user information,” Google Transparency Report, n.d. https://transparencyreport.google.com/user-data/overview (accessed July 9, 2020).

52. Robert Atkinson et al., “A Policymaker’s Guide to the ‘Techlash’—What It Is and Why It’s A Threat to Growth and Progress,” ITIF, October 28, 2019, https://itif.org/publications/2019/10/28/policymakers-guide-techlash.

53. “Statement from Attorney General William P. Barr on Introduction of Lawful Access Bill in Senate,” U.S. Department of Justice, June 23, 2020, https://www.justice.gov/opa/pr/statement-attorney-general-william-p-barr-introduction-lawful-access-bill-senate.

54. “A new law intended to curb sex trafficking threatens the future of the internet as we know it,” *Vox*, July 2, 2018, https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.

55. “Investigatory Powers Bill,” U.K. Parliament, 2016, https://publications.parliament.uk/pa/bills/lbill/2016-2017/0066/17066.pdf.

56. Sharon Franklin et. al., “Open Letter to GCHQ on the Threats Posed by the Ghost Protocol,” Lawfare, May 30, 2019, accessed July 30, 2019, https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal.

57. “Assistance and Access Bill 2018,” Australian Government, August 2018, accessed July 16, 2019, https://assets.documentcloud.org/documents/4756738/Explanatory-Document.pdf.

58. Brittany Bieber et al., “Civil Liberties Vs National Security in the Encryption Debate: Exceptional Access and the Trust Deficit,” Cyber Security: A Peer-Reviewed Journal, Vol. 2, No. 4, Summer 2019, 360-386, https://www.ingentaconnect.com/content/hsp/jcs/2019/00000002/00000004/art00008.

59. Ibid.

60. Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," *Schneier on Security*, February 2016, accessed July 23, 2019, https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf.

61. Joan Daemen and Vincent Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard* (Springer: Germany, 1998), https://autonome-antifa.org/IMG/pdf/Rijndael.pdf.

62. Lance J. Hoffman et al., "Cyberspace Policy Institute, Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations," June 10, 1999, https://www.cryptome.org/cpi-survey.htm; Jay Stowsky, "Secrets or Shields to Share. New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age," BRIE Working Paper 151, 2003, https://escholarship.org/uc/item/89r4j908.

63. W. Kuan Hon, *Data localization Laws and Policy: The EU Data Protection International Transfers Restrictions Through a Cloud Computing Lens* (Northampton, MA: Edward Elgar Publishing, Inc., 2017).

64. "Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018," Submission by the Department of Homeland Affairs, Australian Government, to the Parliamentary Joint Committee on Intelligence and Security, July 2019, https://www.aph.gov.au/DocumentStore.ashx?id=8aecf13f-bc77-4f25-a867-b1708949c095&subId=668072 (accessed November 19, 2019).

65. The Clinger Cohen Act of 1996 directs the federal government to acquire IT from the private sector. 40 U.S.C. § 1401, Clinger Cohen Act, *Justia*, http://law.justia.com/codes/us/1996/title40/chap25/sec1401.

66. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law," Information Technology and Innovation Foundation, March 14, 2016, https://itif.org/publications/2016/03/14/unlocking-encryption-information-security-and-rule-law.