ITIF
INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Unlocking Encryption: Information Security and the Rule of Law

BY DANIEL CASTRO AND ALAN MCQUINN | MARCH 2016

Advancements in the field of information security, particularly in how to use encryption to protect the confidentiality of information, have vastly improved security for consumers and businesses. But as products and services have become more secure, it has become harder for law enforcement and national security agencies to access some information that could help them prevent and investigate crimes and terrorism.[1] This has created one of the most difficult policy dilemmas of the digital age, as encryption both improves security for consumers and businesses and makes it harder for governments to protect them from other threats. There is no way to square this circle, so any choice will come with tradeoffs. However, ITIF believes that the U.S. government should not restrict or weaken encryption, because any attempts to do so would reduce the overall security of law-abiding citizens and businesses, make it more difficult for U.S. companies to compete in global markets, and limit advancements in information security. Moreover, attempts to restrict or weaken encryption would be ineffective at keeping this technology out of the hands of many criminals and terrorists.

Advances in information security could lead to tradeoffs in the effectiveness of law enforcement, but limiting encryption will certainly make the average consumer and business less secure.

Cybersecurity is often portrayed as a never-ending arms race pitting those who wish to secure their computers and networks against attackers intent on breaking into their systems. But while the two sides do indeed engage in a continuous back-and-forth, especially around new technologies, it is not true that cybersecurity has reached a stalemate. Researchers have been steadily improving their knowledge of how to effectively secure electronic data. The past few decades have seen a stream of advancements in encryption and many companies have integrated these advancements into their products and services to improve security for consumers and businesses. As such, encryption has become a fundamental component of improving cybersecurity, and law enforcement, civil society, security experts, and even the president of the United States all agree on its benefits.[2]

But as the methods that citizens and businesses use to secure their information have evolved, some government agencies have pushed back against these improvements, citing national security concerns. Government efforts to limit encryption have had various levels of success in restricting wider use of secure technology.[3] Some of these efforts have been conducted publicly, such as the much-maligned Clipper Chip proposal in the 1990s.[4] Other attempts were clandestine, generating distrust among the general public, foreign governments, and industry stakeholders. One example is the National Security Agency's (NSA) surreptitious efforts to manipulate certain cryptographic standards, introduce backdoors in U.S. products, and hide security vulnerabilities it has discovered in commercial systems so that the government could exploit those weaknesses.[5] These types of secretive actions have weakened data security for both U.S. firms and consumers and left the security products they use susceptible to attacks. The U.S. government's surveillance efforts have also sowed the seeds of distrust around the world, damaging U.S. IT competitiveness.[6]

Recently, some law enforcement agencies have renewed the debate about privacy, security, and the rule of law in the digital age, following the decision by a number of mobile and cloud-based service providers to upgrade their security controls so that customers retain the keys used to encrypt data, thereby preventing third parties, including the companies and law enforcement, from accessing their data. (Throughout this report, we will refer to this type of encryption as "client-side encryption" and "end-to-end encryption.") As a result, there is new urgency on the part of law enforcement and the intelligence community to limit the spread of encryption. In the past, the use of encryption was not as pervasive as it is today, in part because the computing power necessary to securely encrypt and decrypt data was expensive. But with covert techniques less politically tolerable today, as well as a growing awareness that brute-force techniques cannot be used to break into secure systems, some members of law enforcement, such as the Federal Bureau of Investigations (FBI), are calling for companies to control a separate set of encryption keys, independent of the user's keys, to access customer data with a court order.[7] In addition, the FBI has called for companies to help law enforcement hack into their devices. Most notably, the FBI has asked Apple to modify the security features in the software installed on the iPhone of a deceased terrorist suspect so that federal investigators can attempt to break into the device.[8] These proposals have met strong opposition from civil liberties organizations, security experts, the technology industry, and even some former members of law enforcement and the intelligence community.[9]

Unfortunately, some advocates on both sides have become entrenched, seizing upon imprecise arguments to justify their respective stances. Critics on one side conflate all of law enforcement's needs and proposals into a single, kneejerk assertion that anything it does to limit encryption will destroy cybersecurity and privacy, while many on the other side claim that weakening encryption has no real cost to consumers and businesses.[10]

This report will examine the nuances of each of the U.S. government's arguments and proposals to limit the use of encryption and analyze their benefits and trade-offs. The report begins by describing the basics of encryption, how it has evolved, and how law enforcement and intelligence agencies have sought to gain access to encrypted data over time. Second, the report analyzes the various methods that governments could use to limit encryption and their tradeoffs. Third, the report assesses the current debate, including the arguments and proposals that the U.S. government has publicly advocated. Fourth, the report discusses the potential consequences of limiting encryption for U.S. businesses and consumers, government actors, and the digital economy.

The report concludes that the U.S. government should not limit the commercialization of cybersecurity innovations, especially encryption. Doing so is unlikely to have a significant impact on the ability of terrorists and sophisticated criminals to engage in encrypted communications, but it will make the average consumer and business less secure, preclude much advancement in information security and system architecture, and harm the competitiveness of U.S. companies, costing U.S. jobs. Instead, policymakers should encourage information security at home and abroad through the following policies:

- Congress should bar the NSA from intentionally weakening encryption standards and strengthen transparency in those processes.
- Congress should pass legislation banning all government efforts to install encryption backdoors or require companies to alter the design of the systems they sell to allow government access, preempting states' actions on these issues.
- Congress should pass legislation requiring all federal agencies that discover security flaws to disclose them in a timely and responsible manner, and to work with private industry to fix them.
- Congress should examine whether U.S. courts can better balance the interests of the individual and the state by allowing law enforcement to hold suspects in contempt of court for failing to disclose encryption keys to their own encrypted data.
- Congress should provide additional resources to federal, state, and local law enforcement for cyberforensics.
- Congress should establish clear rules for how and when law enforcement can hack into private systems, and how and when law enforcement can compel companies to assist in investigations.
- U.S. trade negotiators should oppose foreign governments' efforts to introduce backdoors in software or weaken encryption, including rules to require companies to sell products with weak encryption.
- The U.S. government should promote cybersecurity around the world by championing strong encryption in global Internet and technology policy forums.

THE EVOLUTION OF ENCRYPTION

To fully understand this debate, it is helpful to assess how encryption has evolved over time as information technology has improved and as new marketplace needs have emerged. Moreover, some forms of encryption are no longer secure, just as some methods for breaking encryption have become more effective over time. Throughout this process, law enforcement and intelligence agencies have continuously pushed to limit encryption to retain access to information.

Symmetric Encryption (1960s-Present)

In the late 1960s, as businesses started to use computers to share and store information in digital form, they needed a way to easily secure that information.[11] These first forms of commercial encryption used symmetric key algorithms, which means the sender and receiver use the same cryptographic key for encryption and decryption, respectively. An analog to this type of encryption is a mechanical lock with a single key that can lock and unlock it.

Throughout the 1970s, the NSA continuously pushed to limit encryption research.

Private-sector and academic efforts to develop better encryption received pushback from intelligence agencies that feared the increased prevalence of encrypted information would limit their ability to view digital communications. Indeed, until this time, it was governments that had used encryption, principally for military reasons.[12] When storing data locally with symmetric encryption, only the individuals holding the key can decrypt the data. Thus, government agencies and other third-parties cannot access the data, nor can the government compel third-party key holders to turn over the key. Instead, governments would have to acquire the key from the source of the data, just as they have to do today with other forms of client-side encryption. In response to non-government developments in encryption, and seeking to keep advances in cryptography a state secret, the National Security Agency (NSA) attempted to control early advances in encryption.[13]

In the late 1960s, more businesses began to research encryption. For example, IBM set up a research group to create an encryption method for a cash-dispensing system that the company was developing for a bank in London.[14] The encryption algorithm created was called "Lucifer," which encrypted 128-bit blocks of data with a 128-bit key.[15] This project came at just the right time for IBM, because in 1968 the U.S. National Bureau of Standards (NBS, now NIST) began researching potential needs for computer security for both the public and private sector.[16] In 1973, NBS announced plans to develop a national standard for encryption of commercial and sensitive yet unclassified government computer data.[17] To this end, NBS sought proposals from the private sector for a public, interoperable standard for data encryption that was adaptable and cost effective.[18] NBS eventually accepted IBM's submission and it became known as the Data Encryption Standard (DES).[19] Unfortunately, the NSA interfered with the process, tampering with the strength of the original algorithm and reducing the key length to 56-bits, in order to make it easier to decrypt.[20] The final version of DES was considerably weaker than the earlier version of Lucifer that IBM had proposed.

Around the same time, academic research in encryption became more common in universities across the United States.[21] Here too, the NSA sought to slow public development of encryption by limiting research. First, the NSA attempted to take control of funding for encryption research from the National Science Foundation.[22] 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 publically.[23] For example, in 1977, when Professor George Davida of the University of Wisconsin, and 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.[24] 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.

Despite these moves to limit public dissemination of encryption, academic institutions continued to publish their findings.[25] Later, court decisions would uphold these academics' right to conduct and publish research on cryptography and ended the NSA's attempts to muzzle them.[26] The result of this research was a boom in security start-ups, such as RSA Security in 1978, which grew from research published at MIT.[27] In addition, as personal computers became popular during the 1980s, a community of researchers, users, and developers grew around creating secure cryptography. This led to the market demand for encryption to be integrated into products throughout the 1980s. For example, in 1983, Lotus Corporation added encryption to "Lotus Notes," an electronic messaging service used primarily by businesses.[28]

As computers got faster and cheaper, so too did methods for breaking into encrypted data by using brute-force attacks—a method in which an adversary tries each possible key until the correct one is found. For example, in 2002, the Electronic Frontier Foundation and Distributed.Net cracked DES in less than twenty-four hours with a machine that cost $250,000.[29] The need for a stronger form of encryption also led the National Institute of Standards and Technology (NIST), which changed its name from NBS in 1988, to replace DES with a new encryption standard known as the Advanced Encryption Standard (AES) in 1997.[30] AES is another symmetric algorithm with key size up to 256-bits, which the NSA deems strong enough to protect top-secret communications.[31] Security experts also began to design security features to make brute-force attacks more difficult. For example, a system could limit the rate or total number of login attempts to prevent automated brute-force attacks.

The biggest limitation of symmetric key algorithms like DES and AES is that they are poorly suited for sharing information securely between multiple parties. This is because it can be difficult to securely distribute keys, as the same key is used to both encrypt and decrypt the information. In the past, for example, it was not a problem to share keys through a trusted courier or during a face-to-face meeting, but a vulnerability arises when the key is sent electronically. Indeed, if it were easy to securely share keys, then the communicating parties would not need encryption, for they could just exchange information directly. While symmetric key encryption is still widely used today, later innovations helped address some of its weaknesses.

Public Key Encryption (1990s-Present)

The limitations of symmetric encryption became more pronounced in the 1980s and 1990s as academics and businesses needed to securely communicate with others on public networks but had no easy way to distribute keys. Indeed, the rise of the commercial Internet exacerbated this problem and helped lead to the introduction of a form of asymmetric encryption called public key encryption. Public key encryption uses two keys, one public and one private.[32] The public key can be shared freely, and it is used to encrypt messages that only the private key can decrypt. While the mathematical solution for this type of encryption dates back to the late 1970s, it was not until the mid-1990s that computer and networking hardware were sufficiently advanced to make an implementation cost-effective.[33]

HOW PUBLIC KEY ENCRYPTION WORKS

With public key encryption, neither party needs to meet in order to exchange information securely.

- Bob wants to share a secret with Alice.
- Alice has a private key *X* and a public key *Y*. Everyone can see Alice's public key, but only she has access to her private key.
- Bob creates a large, random number *N*, which is a symmetric key.
- Bob uses Alice's public key *Y* to encrypt *N* and sends *Y(N)* to Alice.
- Alice uses her private key *X* to decrypt *Y(N)* to get *N*.
- Now both Bob and Alice have the symmetric key *N*, and they can use it to decode any information they send between them. Any third party observing the above exchange would be unable to determine *N*.

After the Internet became commercialized, in 1994, Netscape developed the Secure Sockets Layer (SSL), a cryptographic protocol designed to let servers and clients communicate securely over the Internet.[34] SSL, and its successor Transport Layer Security (TLS), use public key encryption. Interestingly, one of the reasons that the TCP/IP protocol (the technical standard used to network all of the computers on the Internet) did not have encryption integrated into the standard from the beginning is that the NSA had opposed making strong encryption available on public or commercial networks.[35]

Encryption has become fundamental to security on networks like the Internet, and it is used in every industry to securely store and transmit confidential data. Without encryption, consumers would not be able to use popular online services, such as online shopping and banking, nor to securely access any online service requiring a password, such as web mail, social networks, and patient portals.[36] As the cost of encrypting data has fallen along with that of computing power, more and more websites are encrypting all traffic so that a third party cannot intercept any exchanged information. As of April 2015, 29 percent of all Internet traffic in North America was encrypted.[37]

The Crypto Wars (1991-1999)

Until the 1990s, intelligence agencies had primarily resisted the public dissemination of encryption out of the fear that its widespread use would make it more difficult to conduct surveillance of electronic data and communications. Law enforcement agencies joined these efforts in the 1990s as relatively low-cost computers gained enough processing power to be capable of encrypting data with a level of security that would make it nearly impossible for the government to break. As these devices grew in popularity, law enforcement officials feared the technology would foil their investigations. Later, the FBI's former General Council Valerie Caproni would dub this problem "going dark."[38]

Throughout the 1990s, the U.S. government used two tactics to control encryption: mandating key escrow systems and limiting exports.[39] First, in 1991, the NSA promoted legislation that would force 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] Congress refused to pass this legislation. 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.[41] In 1993, the NSA 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.[42] Under the initial scheme, the U.S. Department of Treasury's Automated Systems Division and NIST would hold escrowed keys.[43] 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.[44]

The U.S. government also maintained restrictions on the export of encryption. Since WWII, the U.S. government had strictly controlled the export of encryption for national security reasons. As early as 1954, Congress enacted legislation to restrict export of weapons and munitions, and in 1976 Congress delegated authority over export controls for encryption to the president.[45] Since then, the State Department has limited export of virtually every piece of encryption software and related technology under the U.S. Munitions List, which imposed stringent controls on commercial encryption products, with only a few exceptions.[46] In December 1996, President Bill Clinton loosened export prohibitions on products using encryption, as long as the encryption used a comparatively weak key size of less than 56 bits, which meant that companies still could not export products with advanced encryption.[47] This persisted until 1999 despite the fact that researchers around the world studied advanced forms of encryption and foreign companies freely offered products with stronger forms of encryption. As a result, foreign companies—such as F-secure in Finland, Trend Micro in Taiwan, and Checkpoint and Aladdin in Israel, to name a few—gained significant market advantage throughout the world, including in the United States, at the expense of U.S. companies.[48]

Throughout the decade, technologists, cryptographers, civil-society groups, and the tech industry objected to the U.S. government's interference with the dissemination of encryption and voiced their support for strong encryption to policymakers.[49] In the early 1990s, a loose group of computer hackers, libertarians, and hardware engineers known as the "CypherPunks" formed to push back on government interference with cryptography.[50] Separately, in response to concern that the U.S. government would limit access to encryption in 1991, an engineer named Philip Zimmermann created Pretty Good Privacy (PGP), software that allowed individuals to communicate securely.[51] The software used a minimum of 128-bit keys and depended on a web of trust—which does not require a centralized authority to authenticate users, instead relying on trust relationships between users themselves.[52] After Zimmerman published his software and the Cypherpunks helped distribute it, the U.S. government investigated him for violating export controls, but dropped its case in 1996, shortly before issuing new regulations.[53]

In 1999, the Ninth Circuit of Appeals helped strike down the government's restrictions on exporting encryption. In *Bernstein vs. U.S. Department of Justice*, the court decided "efforts to control encryption thus implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty."[54] In response to the *Bernstein* decision, growing pressure from industry and advocacy groups, and the European Union's decision to loosen its own encryption export controls, the U.S. government eventually relaxed its encryption export controls. Finally, this debate over the use of strong encryption and efficacy of government-mandated key escrow, referred to as the Crypto Wars, came to an end.

The Crypto Wars resulted in the understanding that restricting encryption by limiting its spread and controlling its strength was bad policy.

In light of this debate, the U.S. federal government decided that restricting encryption by limiting its spread and controlling its strength was bad policy. It was not only the CypherPunks who fought for the benefits of encryption, but computing, telecommunications, and financial institutions that relied on encryption protections and did not want their global computing infrastructure compromised by a government-mandated key escrow system. These parties saw the benefits of making encryption public and widely available to everyone. And by the end of the century, critical infrastructure such as water plants, telecommunication's facilities, and privately operated nuclear energy facilities, also relied on the strongest possible methods of encryption to ensure its protection.[55] As former Deputy Secretary of Defense John Hamre said in 1999:

> "We in the Defense Department [supported the new policy] because I think we feel the problem more intensely than does anyone else in the United States… We are just as vulnerable in cyberspace as is anybody, and we strongly need the sorts of protections that come with strong encryption."[56]

The Cloud Computing Era (1999-Present)

In 1999, Salesforce.com brought the concept of cloud computing—delivering scalable computing resources as a service—to the masses.[57] Other companies, such as Amazon and Google soon followed suit, and today a growing number of consumers and businesses use cloud-based applications and services.[58] However, many of these initial cloud-computing applications introduced a new security vulnerability, since consumers and businesses often no longer maintained exclusive control of their data—rather, in many cases the cloud provider also has access to the customer's data.[59]

Before cloud computing, a company would encrypt its own data and maintain its own key to ensure security. But in order to use many cloud services, the cloud provider needs to have access to the information in order to store and process it. Therefore, while the communications between customers and their cloud service provider are encrypted, customers no longer have exclusive access to their data. As a result, law enforcement and intelligence agencies can circumvent encryption by having the service provider turn over the customer data. In addition, consumers have less control of their security and there is increased risk for consumer data in cloud systems. Cloud providers are not immune to data breaches. For example, Code Spaces—a code hosting and software collaboration platform—suffered a data breach through its third party cloud provider due to password mismanagement.[60]

Not surprisingly, cloud computing providers have been working diligently to close this security gap so that cloud-based offerings have the same, if not better, level of security as non-cloud solutions. They have introduced end-to-end encryption—where only the endpoint computers hold the keys—so that data is continuously protected from its origin to its destination and so that no third-party has access to a private key. For example, Apple has continuously updated its cloud encryption standards for its devices and services, such as by encrypting iCloud email.[61] Similarly, Amazon Web Services (AWS) offers its customers a variety of different security sharing options for data stored in the cloud, whether they want to full or partial control of their encryption keys and key management infrastructure, or choose to cede full control to AWS.[62] Other security measures were aimed at fixing human error rather than improving technology. For example, in response to hackers accessing a cache of celebrity photos through their iCloud accounts, Apple announced plans to keep hackers out of its customers' accounts through a notification regime and two-factor authentication.[63]

Securing Mobile Devices (2000s-Present)

Companies have also been working to steadily improve the security of mobile devices through encryption. Throughout the 2000s, as increasing numbers of people bought smartphones—devices that combine the functionality of mobile phones with personal digital assistants (PDAs)—criminals started targeting the new technology to either steal or for fraud or identify-theft purposes. Early forms of mobile malware data back to 2004, when criminals developed malware for mobile devices that would send text messages at premium rates, putting fraudulent charges on the victim's bill.[64]

In recent years, these problems have escalated. Smartphone theft has become an epidemic in the United States with over 1 million smartphones stolen each year.[65] In addition to profiting off the sale of the device, many thieves who steal mobile devices attempt to target the phone's data. In one study, researchers intentionally lost 50 smartphones with simulated personal and corporate data on them, installing a report monitoring mechanism to analyze what people would do to them when they were found.[66] They found 95 percent of those who found a device accessed its sensitive information, but only 50 percent of those individuals tried to get in touch with its "owner" to return the device, despite the fact that the owners' contact information was prominently displayed.[67]

By protecting a phone so that only the owner can use it, many companies hope to remove thieves' incentive from stealing it in the first place. In 2014, several major tech companies announced that their new smartphone operating systems would automatically encrypt data stored locally and communications sent through messaging apps, via a user-generated encryption key unknown and unknowable to the company, making it impossible for the company to comply with law enforcement warrants for communications on their products.[68] For example, Apple updated its messaging app on its latest batches of device software to allow users to control their encryption keys and communicate securely without the company having access by default.[69] Google, likewise, offers encryption options in its Android messaging software for smartphones.[70]

Many mobile device manufacturers are also enabling full disk encryption (FDE) by default on their products. FDE is a type of encrypted storage whereby all data on a device is automatically encrypted so that only a person with proper authentication can decrypt it, and keys are stored locally to that device.[71] Some devices allow users to authenticate using biometrics, such as a fingerprint or facial recognition. This means that if the device is lost or stolen, the data is still protected unless someone has the key or password. In some cases, companies have added additional anti-theft mechanisms to protect user data, such as erasing the device after too many failed login attempts.[72]

The Internet of Things (Present and Beyond)

Many other devices are increasingly being connected to the Internet. The Internet of Things refers to the idea that the Internet is no longer simply a global network for people to communicate with one another, but also a platform by which devices are embedded with Internet-connected sensors that enable them to communicate electronically with the world around them.[73] Connected devices are starting to be incorporated in homes with products such as smart thermostats and smart lighting; in cars to provide navigation, driving safety, and maintenance; and even on individuals' bodies, such as with wearable devices that help individuals manage their health and fitness.[74] Gartner estimated that 6.4 billion objects will be connected to the Internet worldwide this year.[75] Furthermore, it is estimated that the Internet of Things will generate up to $11 trillion per year in economic value by 2025, impacting every aspect of the economy and society.[76]

The prospect of billions of connected devices will lead to an increasingly complex interconnected environment. Researchers are just starting to develop solutions to address the security issues of this complex environment and these solutions will need to change to meet the unique needs of connected devices. Encryption will be necessary to secure all of the information these devices collect, store, and transmit. Like most other technologies, encryption—if left unimpeded—will continue to evolve and improve to address the problems of today, and those of tomorrow.[77]

A NEW CRYPTO WAR?

In response to Apple's and Google's announcements that they would be upgrading their products so that customers would not have to share their encryption keys with a third party, thus effectively limiting the ability of the companies to comply with law enforcement requests, the director of the FBI, James B. Comey, Jr., revived the debate over "going dark" in October 2014.[78] "The law hasn't kept pace with technology, and this disconnect has created a significant public safety problem," Comey said at the time.

Soon, representatives from the Department of Justice, the FBI, intelligence agencies, district attorneys, and other law enforcement agencies came out in favor of key escrow systems in which companies hold an extra set of encryption keys that they can turn over to law enforcement upon lawful request. Director Comey, Deputy Attorney General Sally Yates, and a number of other prominent law enforcement officials testified before Congress arguing that companies must come up with some mechanism to decrypt information if served with a lawful court order.[79] A report from the Manhattan District Attorney's office on smartphone encryption and public safety similarly called for companies to maintain access to encrypted storage and communications on consumer devices, effectively banning client-side encryption.[80] Other prominent politicians and law enforcement officials from around the world have also come out against certain forms of encryption. For example, the prime minister of the United Kingdom David Cameron, in the wake of the Charlie Hebdo attack in Paris, made comments that suggested the UK should ban end-to-end encryption to prevent and solve crimes, saying:

> "…but the question we must ask ourselves is whether, as technology develops, we are content to leave a safe space—a new means of communication—for terrorists to communicate with each other. My answer is no, we should not be, which means that we must look at all the new media being produced and ensure that, in every case, we are able, in extremis and on the signature of a warrant, to get to the bottom of what is going on."[81]

There is new urgency for law enforcement and the intelligence community to limit the spread of client-side encryption.

Cameron called for the government to "modernize" the law and announced intentions to introduce new legislation to give law enforcement this power.[82] Similarly, Rob Wainwright, director of Europol, called encryption the "biggest problem" when combating terrorism.[83] Other voices from former law enforcement and National Security agencies endorsed these efforts as well. For example, Ronald Hosko, president of the Law Enforcement Legal Defense Fund and former assistant director of the FBI Criminal Investigative Division, wrote an article in the *Washington Post* arguing that companies should not encrypt their products by default or make it more difficult for law enforcement to access "data, contacts, photos and email stored on the phone itself."[84]

However, many prominent voices, including computer scientists, business leaders, civil-society groups, and former and current government officials pushed back on proposals to limit encryption, as they had in the 1990s. For example, several computer scientists and researchers wrote a paper in June 2015 explaining many of the security problems with maintaining extraordinary access to encrypted data.[85] Apple CEO Tim Cook has continuously argued against government-mandated back doors, key escrow, and limited encryption by any means.[86] Furthermore, Mike McConnell, Michael Chertoff, and William Lynn—the former director of the NSA, the former homeland security secretary, and the former deputy defense secretary, respectively—penned an op-ed arguing that full, "ubiquitous" encryption provides essential security, and that law enforcement and intelligence organizations' fears were "overblown."[87] Similarly, current NSA director Mike

Rogers, despite past calls to create similar key escrow systems, recently said that arguing against encryption is a "waste of time" and that encryption was "foundational to the future."[88] To be sure, the NSA has not changed its stances on extraordinary access to encryption.[89]

In May 2015, 140 tech companies, prominent technologists, and civil liberties groups sent a letter to the White House to make the case against limits on encryption as the president decided how to address law enforcement's need to access data in a world of increasingly common encryption strategies that give keys to consumers rather than companies.[90] In October 2015, the Obama administration backed away from seeking legislation that would allow U.S. law enforcement to directly access encrypted messages.[91] These groups continued to push, petitioning the White House to affirm its support for strong encryption as its official stance on encrypted communications on its "We the People" site, reaching over 100,000 signatures within 30 days to elicit a response from the administration.[92] As a result, the administration started meeting with civil society groups and technical experts to come to a decision on its position and possible solutions.[93] More recently, another 200 computer security experts, various human rights and civil society groups, and tech companies wrote an open letter to world leaders asking them to reject attempts to put limits on encryption.[94] In response to these efforts, France rejected anti-terrorism legislation that would have mandated company-controlled key escrow systems in manufactured products, and the Netherlands released its official position that it will not require extraordinary access to encryption.[95]

The rash of recent terrorist attacks around the world led many to argue for limiting encryption. Robert Hannigan, the director of GCHQ, cited the widespread use of end-to-end encryption as a boon for terrorists in an article he wrote in the *Financial Times*.[96] These attacks have increased legislative efforts focused on ways the government can force companies to build key escrow systems into their technology to decrypt data if presented with a search warrant. For example, Federal Communication Commission Chairman Tom Wheeler suggested that Congress update the Communications Assistance for Law Enforcement Act (CALEA) to force companies to build key escrow systems.[97] This would be a substantial change as CALEA only applies to telecommunications, does not allow the government to require any specific design changes, and specifically excludes information services.[98]

Senators Diane Feinstein (D-CA) and Richard Burr (R-NC) have vowed to introduce legislation to compel companies to decrypt data for law enforcement officials.[99] Senator John McCain (R-AZ) has also pushed for legislation that would "require U.S. telecommunications companies to adopt technological alternatives that allow them to comply with lawful requests for access to content."[100] Similarly, in February 2016, Rep. Mike McCaul (R-TX) and Senator Mark Warner (D-VA) introduced legislation to create a national commission that will analyze the challenges both the law enforcement and intelligence community face with advances in technology, and issue a report on the impact, role, and future of encryption in the United States.[101] These efforts have also taken hold in several state legislatures, with lawmakers in both New York and California considering legislation to require extraordinary access to encryption in commercial products and services.[102]

HOW ENCRYPTION DISRUPTS INVESTIGATIONS

U.S. law enforcement and intelligence agencies work hard to protect the safety of U.S. citizens and residents. Recent advances in encryption, along with increased adoption, have affected how government agencies protect national security and fight crime by limiting the amount of information they can access. However, law enforcement and security agencies conduct different types of investigations. While national security agencies sometimes surveil large amounts of information, law enforcement investigations typically target information relevant to a specific case. Indeed, law enforcement officials do not have the authority to serve mass warrants.

Figure 1: How encryption affects government access to data-at-rest and data-in-motion.

	Data at Rest	Data in Motion
Law Enforcement	Law enforcement cannot gain access to encrypted data stored on a user's device or in the cloud, even with a search warrant.	Law enforcement cannot use wiretaps to intercept communications.
Intelligence Community	Intelligence community cannot gain access to encrypted data stored on a user's device or in the cloud, including bulk access to user data.	Intelligence community cannot analyze communications for trigger terms.

For investigative purposes, information is categorized as "data at rest" or "data in motion." Data at rest refers to any form of electronic storage, whether on a device or in the cloud. To gain access to data at rest, law enforcement must obtain a court order, a process that requires them to identify the owner of the data and to provide justification to a judge for why they should have access. However, even if they receive access to the data, law enforcement officials will be unable to make sense of the encrypted data if they do not have the key. Similarly, if Internet companies do not have the key to their customers' encrypted data, then they will be unable to comply with a request by intelligence agencies to search through this data.

Data in motion refers to information moving between two or more endpoints. Law enforcement may try to gain access to data in motion through court-ordered wiretaps to monitor specific communications. For example, law enforcement may be able to gain access to messages passed through a messaging service if the service provider can decrypt the communications. However, if the communications are encrypted end-to-end so that only the endpoints have keys, law enforcement officials will be unable to decipher it. To date, this has not been a widespread problem. Federal wiretap data indicates that out of over 32,000 wiretaps conducted to intercept wire, oral, or electric communications from 2001 to 2014, law enforcement only encountered encrypted communications 132 times.[103] However, this number will likely grow as encryption becomes more prevalent. In addition, when national security agencies intercept large amounts of online data in transit to search for trigger terms, they will not be able to access this information if the data is encrypted. If the data is encrypted, intelligence agencies will only be able to see metadata—data that describes information about a communication, such as information on the source and destination of packets and how much and when data are transferred.

While more widespread adoption of encryption will make it harder for law enforcement and intelligence agencies to do their job as they do today, the overall effect it will have on them is unknown. Future tools and techniques might also have an impact on their ability to conduct investigations, and this impact is also unknown and will change over time.[104]

METHODS FOR BREAKING ENCRYPTION

There are multiple methods that a government can use to gain access to encrypted information. Some methods involve breaking encryption, some involve circumventing it, and some involve gaining access to the keys. Some of the tactics rely on covert actions by the intelligence community, so law enforcement will not always be able to directly use these methods. However, since law enforcement may request assistance from the intelligence community, it may still be able to benefit from these capabilities.[105] Some tactics seek to impose broad limitations on encryption, while others are narrowly focused on one business, individual, or product or service. Each of these methods also comes with tradeoffs in the form of different levels of security risk and reliability of access for law enforcement and intelligence agencies.

Banning Strong Encryption

Government can access encrypted information by simply banning encryption above a certain strength or by allowing only weaker forms of encryption that it has the resources to break. This would mean that all products, services, and devices sold or imported into a country would provide a means for its intelligence officials to access stored data through brute force attacks. Because law enforcement often does not have the resources to conduct this sort of time-consuming method of breaking encryption, this method is usually reserved for intelligence agencies. For example, the United Kingdom could pass a law that bans encryption stronger than 64-bit keys, knowing its intelligence agency has the resources to crack any form of legal encryption in the country.

Figure 2: The usefulness of different methods the government can use to increase access to encrypted information.

Method	Usefulness for Government	Impact on Security
Banning Strong Encryption	Banning strong encryption on products and services sold in the U.S. allows the intelligence community to use brute-force attacks to access encrypted information.	Banning strong encryption weakens the security of all products and services, especially from nation-state threats.
Weakening Encryption Standards	Surreptitiously weakening encryption standards allows the intelligence community to use secret attacks to access encrypted information.	Weakening national encryption standards weakens all U.S. encryption products that use those standards, allowing bad actors to also exploit vulnerabilities for access.
Creating Software and Hardware Backdoors	Secretly installing backdoors can allow the intelligence community to circumvent encryption, often without notifying the user.	If backdoors are discovered by malicious actors, they can exploit these vulnerabilities.
Government Hacking	The government can attempt to hack into products or services, but it has no guarantee of success.	Government hacking can create new vulnerabilities which other attackers could exploit.
Mandatory Key Escrow	Key escrow allows the government to use a court order to unlock encrypted information by forcing companies, a neutral third party, or the government itself to store an extra key to all encrypted data.	Requiring key escrow exposes businesses and consumers to additional risks from security breaches and precludes certain security features, such as perfect forward secrecy.
Prohibiting Client-Side Encryption	By not allowing users to encrypt data using their own keys, the government can access data through third party service providers.	User data can be exposed if data is stolen or leaked by a third party. Ultimately, the security of users' data is dependent on the actions of the service provider.
Traditional Methods of Obtaining Information	Traditional methods, such as surveillance, witnesses, physical searches, or confessions, to learn encryption keys vary in effectiveness.	There is minimal impact on security.

The security ramifications of this move would be dire, weakening the security of all products and services produced or imported into a country, especially against attacks from sophisticated hackers or nation states. To date, no country has created plans to completely ban encryption above a certain strength. Instead, countries have exercised this type of ban narrowly, directing it at devices or services that use encryption their intelligence agencies are unable to bypass. For example, Saudi Arabia and the United Arab Emirates banned the secure messaging function of Blackberry mobile devices in 2010.[106] Similarly, in 2011, Pakistan banned all encryption software and ordered Pakistani Internet Service Providers to tell the government if it caught customers using virtual private networks—networks that use encryption to allow Internet users to browse the web privately.[107]

Weakening Encryption Standards

Intelligence agencies can secretly manipulate and weaken national standards for encryption, with the goal of limiting encryption products and services that use those standards. While these processes are public, intelligence agencies can surreptitiously manipulate them. This usually requires cross-government participation. In some cases, intelligence agencies can weaken the encryption strength of the national standard, such as the NSA's edits to the U.S. National Bureau of Standards' final DES algorithm.[108] In other instances, intelligence agencies can manipulate national standards to leave security flaws in the final algorithm. For example, the Snowden revelations exposed that the NSA had surreptitiously circumvented encryption used to secure digital communications by manipulating a cryptography standard that the National Institute of Standards and Technology (NIST) had issued in 2006.[109] This allowed the NSA to access data on a product or service using this standard, but also exposed these products and services to abuse by bad actors.[110] As a result, NIST published guidelines discouraging companies from using these standards and promised to give the public an opportunity to provide input on revising new standards.[111]

By compromising an encryption standard that the government uses, and by extension, that much of the private sector will likely use, intelligence agencies would create a vulnerability that malicious actors could discover and exploit. These security flaws could persist for years before the government fixes the issue in a revised standard. For example, security researchers discovered the security flaw in the NIST cryptography standard as early as 2007, but NIST did not revise the standard until 2014.[112]

Creating Software and Hardware Backdoors

Intelligence agencies can create backdoors, gateways giving a third party extraordinary access to a secure product—whether it is hardware (e.g., a physical access port) or software (e.g., code in a computer program). Governments create backdoors to allow direct access to encrypted communications or storage without tipping off their target to the surveillance. Once installed, backdoors can be very effective for intelligence agencies, which gain secret access to devices or systems. However, backdoors are kept secret, which means they are typically only available to the intelligence community and not law enforcement.

Intelligence agencies can also create backdoors in products using encryption, either by forcing companies to build backdoors into their systems for direct access or by surreptitiously installing them on devices. For example, the Snowden revelations revealed that the NSA intercepted routers, servers, and networking equipment made by Cisco while the equipment was in transit so it could secretly insert backdoor surveillance tools without the company's knowledge.[113]

If a backdoor is discovered by adversaries, they can exploit these vulnerabilities, and because backdoors are installed secretly, businesses often do not detect them for long periods of time. For example, in 2015, Juniper Networks, a tech company that produces networking equipment for corporate and government systems, discovered two unauthorized backdoors into its products, including one that allowed adversaries to decrypt traffic—and the culprit of this breach is still unknown.[114] These security flaws on Juniper devices went undetected for three years.[115] Upon close inspection, security researchers discovered that this backdoor was created based on code from the NIST cryptography standard that the NSA had compromised.[116] While Juniper did not use the specific corrupted parameters in its firewall, the overall backdoor effort by the NSA laid the groundwork for someone to attack this system. Because backdoors are targeted at a specific company, person, or products or services, the impact is less than encryption bans or weakened national standards, which can limit encryption for many products and services.

Government Hacking

The government can conduct attacks to break encryption, with or without help from companies. While this is often done by intelligence agencies to install backdoor access to devices, it can also be used to for law enforcement activities. When law enforcement or intelligence agencies attempt to break into a product or service, they have no guarantee of success. Therefore, different types of attacks vary in effectiveness based on what type of encryption a target is using and if a company is working with law enforcement.

Law enforcement officials have used many forms of hacking to find criminals, especially where criminals have used software to encrypt or obscure their online activities. In fact, the FBI not only has its own proprietary surveillance software, it also uses popular hacker tools.[117] One example of this is phishing, where law enforcement masquerades as a trustworthy source over an electronic communication to get someone to download surveillance software. This happened in 2007 when the FBI sent a fake news article to the anonymous email address associated with repeated bomb threats; downloading the article installed surveillance software that, when clicked, revealed the suspect's identity.[118]

Another common tactic is installing a keylogger, software that is designed to secretly record keystrokes. Keyloggers can be used to intercept passwords or other sensitive information typed into a computer. For example, in 2007, the U.S. Drug Enforcement Administration used a keylogger to bypass PGP and an encrypted email service by monitoring suspects' keystrokes for their passwords.[119] In order to use a keylogger, law enforcement must gain surreptitious access to the encrypted device, something that can be difficult during an active investigation.

The intelligence community has also hacked into private companies to facilitate surveillance on the customers of those companies. For example, in 2010 the NSA and the U.K. Government Communications Headquarters (GCHQ) allegedly used malware to hack into the computer systems of Gemalto—a leading manufacturer of SIM cards based in the Netherlands—to steal the encryption keys for millions of SIM cards.[120] Documents associated with the case contain information pertaining only to three months of access by NSA and GCHQ, but surveillance may have continued after that time.[121]

The government can also ask or force a company to conduct attacks on its behalf. For example, for end-to-end encryption communications systems that depend on centralized, provider-operated key servers (e.g., WhatsApp), the government can attack key distribution, forcing companies to distribute illegitimate keys or register devices that store and receive information related to a user's account.[122] In this instance, when a user tries to send a message over an encrypted network, he or she must communicate with a key server that tells the user the public key of the intended recipient. At this point, if the government forces a company to substitute its own keys in addition to the intended public keys of the recipient, it can also gain access to the information.

Similarly, the government can work with a company to remove the security features in the devices or services it provides to certain customers. For example, in the San Bernardino case, the FBI asked Apple to create a special version of its software where the safeguards that make it difficult to attempt to hack the iPhone using brute force methods are disabled and then load this software on to the suspect's phone.[123] These types of software updates must typically be signed by a private key held by the software maker for them to be accepted by the device.

As with installing surreptitious backdoors into products and services, there are tradeoffs with other forms of government hacking. Hacking a device that is still in use, such as by installing malware, can create new vulnerabilities that other attackers could exploit. And some methods, such as introducing vulnerabilities through automatic software updates, could discourage consumers from patching security vulnerabilities on their devices. And even when the government does not introduce new vulnerabilities, if it does not responsibly disclose vulnerabilities it discovers to the private sector, it allows these weaknesses to persist—so that they could later be exploited by bad actors.

Mandatory Key Escrow

The government can also require key-recovery mechanisms, commonly referred to as "key escrow." In these systems, in addition to the original key used to encrypt and decrypt information, there is a second key that is held by a third party. With key escrow, there is no portal for direct access, such as a secret backdoor. Instead, the software is designed to create an extra key for the third party, such as the company offering the service or the government. When law enforcement wants to intercept encrypted data or gain access to a device, the key held in escrow can decrypt them.

Key escrow systems, if widely adopted, would be an effective tool for law enforcement to gain access to encrypted information. By acquiring a warrant or court order, law enforcement could compel a company to decrypt communications without the knowledge of the people using the service. Law enforcement and the Obama administration have discussed a number of ways to implement this type of key escrow system.[124] For example, device makers could be required to maintain a separate set of keys that would allow access to encrypted data over a physical port on the devices. If law enforcement officials have physical access to the device, they could then extract the encrypted data after using a court order to obtain the key. The administration also proposed a "forced back-up" plan whereby companies with the capability would be required to automatically upload customer data, before it is encrypted, to a location where the government could later access it. Both of these proposals would only address encrypted storage rather than encrypted communications. Finally, other prominent voices, such as NSA director Mike Rogers, proposed split-key encryption, where multiple parties each control a partial key, and all parties must come together under a court order to decrypt the information.[125] While this approach would limit the risk of exploitation by requiring an attacker to obtain multiple partial keys to recover a full one, it still introduces a vulnerability—all keys must come together at once to decrypt the information and the keys must remain the same across multiple transactions. In none of these scenarios would the government be able to access all encrypted data, as users could still use third-party software to encrypt their information prior to using a communication service or storing it on a device.

But while these systems can be beneficial to law enforcement, they would also have a negative result: Key escrow takes away from individuals the power to secure their own data in favor of a much less secure overall encryption framework. There are several problems with key escrow systems.[126] First, these systems increase overall complexity in the system. In a hypothetical key escrow system, a law enforcement request for a company would need to go through several stages to be fulfilled, including authenticating the court's warrant, finding the correct data, locating the correct key in the company's escrow, and retrieving the data from only the time period on the warrant.[127] The company would then need to convert the data into the correct format, transfer it to only authorized and authenticated law enforcement parties, and maintain the ability to audit these requests. Each of these steps adds a new level of complexity and each one is subject to attacks from adversaries—whether it is impersonation attacks like falsifying court documents, insider attacks from rogue employees, or hackers targeting the system that maintains the keys in escrow.

Adding extraordinary access complicates encryption. Every line of new code is a place where a mistake can be made and a flaw produced.

In addition, there are likely billions of encrypted communications created every moment, each with its own set of changing keys.[128] It is simply infeasible to create a system where all of these communications have a system in place that would allow third-party access without adding enormous complexity. Encrypted data is most secure if only those entities that need access to the keys have this access. Adding new keys complicates the system as every line of new code is a place where a mistake can be made and a flaw produced.

Second, key escrow systems end the best practice of "perfect forward secrecy." Unlike traditional encryption systems that use a single key over a long period of time, perfect forward secrecy uses different keys for each encrypted session, known as ephemeral keys. By changing the keys with each new session, an adversary can be prevented from decrypting past or future data if a key used to encrypt information is ever compromised. This minimizes the impact that a bad actor can have on accessing encrypted information. Key escrow ends this practice by mandating that a company hold a master key for all of its communications or an extra set of keys for each individual session. Given the sheer number of keys that perfect forward secrecy generates, it is unreasonable for a public key infrastructure to duplicate and maintain these keys in escrow.

Third, sharing an encryption key with a third party creates new vulnerabilities because there is another point of attack that can be exploited. Past examples of key escrow systems designed to comply with government requests for data have been rife with vulnerabilities. In one example, which became known as the Athens Affair, over 100 senior members of the Greek government had their electronic communications intercepted by still-unknown parties for 10 months during 2004 and 2005.[129] These coopted intercepts were originally built into the Vodafone Greece telephone system to enable lawful access to communications for law enforcement. Similarly, in 2010, a researcher discovered a vulnerability in the infrastructure that Cisco had created for extraordinary access for law enforcement years after it had been introduced and spread to carriers throughout Europe.[130]

A government key escrow system would be even more vulnerable. If a government key escrow system were created, it would also need to be secured. However, virtually no government agency has shown itself to be capable of preventing data breaches, and even the heads of intelligence agencies have had their personal accounts hacked.[131]

Prohibiting Client-Side Encryption

The government could prohibit companies from implementing client-side encryption, whereby consumers control their own encryption keys. By not allowing users to encrypt data using their own keys, third-party service providers will be able to access consumer data to fulfill warrants and court orders. This type of restriction on encryption effectively forces companies to implement their own key escrow systems. Therefore, prohibiting client-side encryption results in the same benefits to law enforcement and risks to consumers as mandating key escrow systems (detailed previously). In addition, this method would not prevent users from using non-U.S. third-party software, or writing their own, which allows them to encrypt data and retain sole custody of the keys.

Ultimately, the security of users' data is dependent on the actions of the service provider, which can create a problem. If a user wants more security, which may increase costs, and a service provider wants to generate profit by decreasing costs, the user may ultimately lose out. However, if users control their own set of keys, then they can secure their data based on the level of risk tolerance appropriate to that data, such as by using stronger keys, changing keys more frequently, and implementing more security measures to limit who can access keys.

Traditional Methods of Obtaining Information

Law enforcement can use other more traditional forms of investigation to gain access to the keys used to encrypt data, including surveillance, witnesses, physical searches, and confessions. For example, law enforcement may secretly observe the password a user enters on a computer or search an office to find paper files containing passwords. These methods of obtaining keys are less useful for intercepting encrypted communications. Many of these methods have been consistently available to law enforcement for decades, and have adapted to changing technologies. For example, before telephones there were no wiretaps, and before transistors law enforcement could not plant listening devices to monitor conversations remotely.[132]

Each of these methods has varying levels of effectiveness. For example, law enforcement can conduct physical searches if it has jurisdiction. Similarly, law enforcement can sometimes compel someone with the encryption key—the sender or receiver of the communication, or the service provider if it has the key—to provide access to decrypted data under certain circumstances.[133] For example, in the case of encrypted phones with biometric locks, such as many new iPhones, law enforcement can sometimes unlock the phone by placing the suspect's fingertips against the phone's fingerprint reader. However, in order for this technique to be feasible, law enforcement must have access to the device and the person. Therefore, law enforcement may not choose to use this method during an investigation if they wish not to be detected. In addition, some of these methods will get more difficult for law enforcement to implement as encryption becomes incorporated into more technologies.

JUSTIFICATIONS AND PROPOSALS FOR ACCESS TO ENCRYPTED DATA

Many law enforcement officials do not want companies to offer any products or services that allow users to maintain full control over the keys used to encrypt their data. Instead, they want companies to operate key escrow systems that would allow them to provide the government access to any customer data. These requests would only be allowed if authorized by a court. Some law enforcement officials have pushed for companies to build these systems voluntarily, while others have proposed legislation.

Law enforcement and national security agency officials have put forth five main arguments to justify their opposition to allowing users to maintain full control of encryption keys:

1. Since law enforcement agencies have always had the ability to access information with warrants, companies should not offer technology that circumvents this process.
2. Without access to encrypted data, the government will be less able to stop or solve crimes and terrorism.
3. Companies have decided to stop retaining a copy of their customers' encryption keys for business reasons alone, not to improve security.
4. Technologists could create a way for the government to access encrypted data without compromising security if they tried harder to solve the problem.
5. At a minimum, companies should help law enforcement officials hack into specific encrypted systems.

Argument 1: Since law enforcement agencies have always had the ability to access information with warrants, companies should not offer technology that circumvents this process.

Some law enforcement officials argue that companies are interfering with their long-standing ability to conduct lawful searches by allowing users to maintain their own encryption keys. These critics caution against a new wave of "warrant-proof encryption," the scenario in which law enforcement goes through established legal processes to obtain information, such as through a search warrant, only to find the information they seek is inaccessible due to encryption.[134] FBI Director Comey made this point when he said, "The core question is this: once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?"[135]

A number of different laws say where and when law enforcement is allowed to execute a search and seizure of data.[136] If these searches are illegal, flawed, or do not meet the standards set forth by any of these governing laws, then law enforcement cannot use any information so obtained to further an investigation. This is because U.S. citizens enjoy a presumptive right to privacy when it comes to searches and seizures under the Fourth Amendment to the Constitution, which can only be violated by law enforcement under certain circumstances. Furthermore, U.S. citizens enjoy protections under the Fifth Amendment, which provides that "[n]o person… shall be compelled in any case to be witness against himself."[137] The Fifth Amendment limits the government's ability to gather evidence by granting individuals the right to refuse to share self-incriminating information. The Eleventh Circuit Court of Appeals has ruled that the Fifth Amendment bars law enforcement from compelling a suspect to provide the key needed to decrypt encrypted data if the key is something the person has memorized, and does not exist in physical form.[138] In the past, this distinction created no problem for law enforcement because a physical lock box or combination safe could be broken into if needed, but there is no "bolt cutter" for encryption. In short, law enforcement agencies have no recourse to access encrypted information. In practical terms, it means law enforcement can compel a suspect to open a biometric lock with a fingerprint, but cannot compel someone to turn over a password.[139]

There are limits to warrants when it comes to encryption. If the FBI issues a warrant to a network operator to decrypt communications sent over its network and the user has encrypted those communications, the company can provide the encrypted packets, but it will not be able to decrypt its content. Similarly, if users encrypt files on their mobile devices, device manufacturers cannot provide law enforcement access to the data. In these cases, law enforcement can only successfully decrypt the user's information if the user provides the key. FBI Director Comey has referred to this situation as "…equivalent of a closet that can't be opened. A safe that can't be cracked."[140]

As a result, there have been several calls to update legislation to allow law enforcement extraordinary access to encrypted materials. For example, New York County District Attorney Cyrus Vance has called for updating the Communications Assistance for Law Enforcement Act (CALEA) to bar companies from providing sole control of encryption keys to their consumers, prohibiting sales of digital devices that cannot be accessed pursuant to a warrant, and examining financial disincentives for companies that do not comply.[141]

Response to Argument 1: Law enforcement officials have never had the ability to read properly encrypted information.

Law enforcement officials have never been able to access certain information. First, law enforcement has never had the power to decrypt data when the user held the key. For example, from the 1970s to 1990s, law enforcement had no practical way to access user data encrypted with DES since no third party controlled the keys, although law enforcement could still obtain court orders to require corporations to turn over their own data.[142] The relatively recent introduction of cloud computing services has created an opportunity for law enforcement and intelligence agencies to circumvent encryption because they can compel the service provider to turn over unencrypted customer data. Second, while law enforcement officials can gain the authority to search any private property, this does not mean that they will always be able to access information sufficiently well-hidden or protected, such as information that is buried in someone's backyard or memorized but never written down.

What has changed is that the use of encryption and digital technologies is significantly more widespread today than in the past; moreover, the users of encryption are increasingly individuals, not just corporations. Thus, while the scale of the impact of encryption on law enforcement is much greater today than in the past, the phenomenon itself—the inability of law enforcement to access encrypted data where the user controls all of the keys—is not new.

Argument 2: Without access to encrypted data, the government will be less able to stop or solve crime and terrorism.

Some law enforcement and intelligence agencies also argue that even if they did not have this level of access to encrypted information before, they need it now to solve crimes and stop terrorism. This has become the case, they argue, because the amount of data that is encrypted today dwarfs what was encrypted in the past. Many people, including criminals and terrorists, use devices and online services that encrypt data. In arguing for extraordinary access to encryption, law enforcement officials have offered three primary categories of crime emboldened by pervasive encryption: common crimes, organized crime, and terrorism.

First, law enforcement argues that if it is unable to access encrypted data, many everyday crimes will go unsolved. Certainly, law enforcement officials can expect to encounter encrypted data more often as consumer devices enable new security features. For example, between October 2014 and June 2015, the office of the New York District Attorney found that 35 percent of the data extracted from phones came from Apple devices and 36 percent came from Android devices.[143] Because these smartphones now enable encryption by default without providing a key to any intermediaries, much of the data on these phones has become unreadable to law enforcement officials. District Attorney Vance pointed to 74 cases involving iPhones between October 2014 and June 2015 in which law enforcement officials could not access a phone's contents.[144] Given that the Manhattan DA's office handles over 100,000 cases each year, this number represents less than a tenth of a percent, but will likely grow over time.[145]

Law enforcement officials have pointed to a series of cases where access to a device was crucial to convicting a criminal, and where, had the devices been encrypted, the case may have gone differently.[146] For example, FBI Director Comey cited a case in which a long-haul trucker kidnapped his girlfriend and drove her from state to state, assaulting her physically and sexually.[147] When the victim escaped, a search warrant for the data on the suspect's phone corroborated the victim's testimony at trial. In New York, a police officer observed a man using a cell phone to film up women's skirts, and upon getting a warrant for the phone, law enforcement was able to discover many images—including those of an under-aged victim—and convict the man.[148] In the absence of other evidence or testimony, law enforcement officials will need access to the perpetrator's unencrypted data in order to prosecute these sorts of crimes.

Second, law enforcement officials have argued that without access to encrypted data they will be unable to prevent organized crime. For example, District Attorney Vance cited the prosecution of an identity theft ring with 29 members who had stolen over 100 American Express credit card numbers and property worth over $1 million.[149] The identity theft ring operated out of restaurants, where waiters would swipe credit card numbers surreptitiously through a card reader to store the credit information. A search of one waiter's unencrypted iPhone revealed text messages that ultimately led to the discovery and prosecution of the illegal enterprise.

Finally, law enforcement officials argue that they need access to encrypted data to fight terrorism. In November 2015, the Islamic State (ISIL) terrorist network targeted Paris, France, with a series of attacks that killed at least 130 people.[150] European officials said that investigations after the event showed these terrorists communicated about the attacks from Syria using encrypted communications.[151] During another terrorism case in San Bernardino, California, in December 2015, perpetrators used Apple devices with encryption to communicate with terrorist groups overseas.[152] As a result of these high-profile cases, some high-level public officials, including Central Intelligence Agency Director John Brennan, and UK Prime Minister Cameron, expressed concern that their countries are facing new and dangerous threats from sophisticated terrorists, justifying limits to the use of encryption.[153]

Law enforcement and intelligence officials argue that in the past, accessing communications has helped them investigate terrorism. In France, for example, investigators took data from smartphones used by terrorists in the Charlie Hebdo attacks and in the attack on a gas facility at Saint-Quentin-Fallavier.[154] Law enforcement officials worry that since encrypted data can frustrate their efforts, terrorists and other criminals will increasingly use these tools to commit offenses and avoid prosecution.

Response to Argument 2: Limiting encryption is not the right answer for stopping crime and preventing terrorism.

Certainly, developments in encryption are likely to impact the effectiveness of law enforcement and the intelligence community, and even more so if they do not develop or use new tools and techniques to investigate crimes and combat terrorism in an age of secure digital communications. However, law enforcement's access to information to prevent and solve crimes always involves a tradeoff with civil liberties. If the U.S. government really wanted to stop domestic terrorism, it could require that every home be installed with a 1984-like two-way screen, where law enforcement computers could listen to every word citizens say. Of course, everyone would rightly react in horror at such a proposal because it gets the balance terribly wrong. Indeed, as the United States transitions into a fully digital economy and society, it will become increasingly important to ensure the security of data.

Given the substantial benefits encryption has to offer, and the likely negative effects of limiting encryption, it is not sufficient to argue that law enforcement's inability to access encrypted materials in its quest to upset various criminal and terrorism investigations justifies extraordinary access to encrypted data. This is so for at least three reasons: 1) accessing encrypted data is not the only way law enforcement officials can fight crime and terrorism, 2) no matter the policy that is put in place, terrorists and sophisticated criminals will still use encryption, and 3) many other legal activities and technologies perpetuate crime.

Accessing encrypted data is not the only way law enforcement can solve crimes.

If criminals could simply avoid prosecution by using encryption, they would have nothing to fear today. However, law enforcement has alternative investigative tools at its disposal, including a steadily growing supply of metadata.[155] Law enforcement has always had multiple investigatory tactics in its arsenal, including testimony from witnesses and collaborators, as well as physical evidence. In addition, law enforcement can use traditional methods of surveillance, as well as commercial technologies like StingRay that facilitate government surveillance of mobile devices.[156] For example, if police can get a warrant to monitor a suspect's home or business, then they may be able to record illegal activity. Law enforcement officials can often get access to metadata. For example, although law enforcement cannot access encrypted messages sent via the popular mobile app Whatsapp, they can use metadata to learn whom particular users are talking to.[157] In the future, law enforcement agencies could develop new tools and methods to further investigations.[158]

To be clear, there are limits to each of these approaches. Law enforcement officials cannot interview suspects if they want to keep an investigation secret. There may not be any intelligence or informants available in a particular case. And metadata might not provide the information law enforcement is seeking.[159]

Furthermore, law enforcement and the intelligence community routinely rely on other methods to stop terrorism, such as international cooperation, domestic intelligence sharing, and following up on tips from informants. For example, in 2009, the Central Intelligence Agency (CIA), FBI, and New York Police Department all worked together to stop an al-Qaeda plan to detonate a bomb on the New York City subway after the CIA shared intelligence on individuals training in foreign terrorist camps with law enforcement.[160] The U.S. Department of Homeland Security's "If You See Something, Say Something" campaign has also helped generate tips from the public.[161] In 2013, the *Wall Street Journal* chronicled nine thwarted terrorists plots in New York since 2002, most of which were foiled by informants. In another case, a tip from an ammunition store clerk stopped a man from repeating the 2009 Fort Hood attack. And, passengers and crew of an airline stopped a suicide bomber in midair, while a relative's tip helped the FBI prevent an attempted bombing in Oregon in 2010.[162]

These approaches will not catch every criminal, and the increased prevalence of encryption will make it more difficult to catch the non-dedicated, non-expert criminal who happens to use an encrypted device.

The U.S. cannot stop terrorists or sophisticated criminals from encrypting data.

Regardless of what laws the U.S. government passes, it cannot stop committed terrorists or criminals from encrypting their data. If bad actors want to use encryption, they can easily find tools to do so from open-source software or foreign providers. Many do so today. An online ISIL tutorial lists the top five "safest" encryption tools for terrorists, and none were made by companies in the United States.[163] A recent survey of 865 hardware and software products incorporating encryption from 55 countries found that two-thirds of these products come from foreign providers and 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.[164] Indeed some of the most advanced work in encryption comes from outside the United States, and the current NIST-approved standard for encryption, AES, was developed by two Belgian cryptographers.[165] Even FBI Director Comey acknowledged the limit of U.S. policy in restricting access to encryption, explaining that any criminal can simply use products and services created outside the United States.[166]

If the United States wants to fully ban certain types of encryption from the hands of these few bad actors, it would need to perform a Herculean feat that would include blocking websites found hosting prohibited encryption tools or code, mandating key escrow systems in all U.S. services, and confiscating devices with prohibited forms of encryption on them at the border.

Moreover, since most of the information about how to encrypt data is available in textbooks or freely online, terrorists or criminal groups can write the code themselves. Many have already. In 2007, al-Qaeda developed software, known as Mujahideen Secrets, to encrypt their online communications.[167] In 2008, al-Qaeda updated the software to strengthen the encryption in response to possible vulnerabilities.[168] 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.[169] In fact, since the NSA leaks, terrorists are likely to use technology created by companies outside the United States.[170] Therefore, if U.S. intelligence agencies make U.S. companies give them extraordinary access to encrypted user data, most terrorists using these tools will likely switch to foreign providers. If this occurs, U.S. law enforcement and security agencies lose access to an important asset: metadata from U.S. providers.

The U.S. should not ban encryption just because it can also be used by criminals. Encryption is an example of dual-use technology. While criminals and terrorists use encryption, the vast majority of its use is by law-abiding consumers and businesses. Many other technologies also allow criminals to commit crimes, such as cars enabling get-away drivers and shovels enabling criminals to bury evidence. The U.S. government should not place limits on encryption just because a small minority of users engage in criminal activity any more than they should place similar limits on cars or shovels.

Argument 3: Companies have decided to stop retaining a copy of their customers' encryption keys for business reasons alone, not to improve security.

Some law enforcement officials, such as FBI Director Comey and Deputy Attorney General Sally Quillian Yates, have argued that companies are engineering systems that deny law enforcement officials access to consumer data for business reasons rather than to improve security.[171] They believe companies are making these changes so that they will be more competitive abroad when selling to customers who do not want the government to access their data.

They also believe that companies have not increased security for their customers by allowing them to maintain the only copy of the keys used to encrypt their data. District Attorney Conley has even argued that since companies gather large amounts of information on their customers for commercial purposes, they should provide access to private customer information for law enforcement purposes. District Attorney Conley said that these companies are "taking full advantage of their customers' private data for commercial purposes while building an impenetrable barrier around evidence in legitimate, court-authorized criminal investigations."[172]

Law enforcement officials have pointed to companies in regulated industries that already use key escrow for their own commercial purposes, or to comply with warrants, as justification for why all companies should implement key escrow systems. For example, FBI Director Comey noted that some industries, such as the financial industry, "have the ability to access the data and comply with court orders, and they are able to do both in a pretty robust way."[173] Similarly, in an article published in the *Wall Street Journal*, Senator Richard Burr (R-NC) cited an example of several major banks using the encrypted messaging service Symphony.[174] When regulators grew concerned that this system would prevent regulators from investigating illegal activities, the banks agreed to store decryption keys with a third party.

Certainly some companies have created key-recovery capabilities as a feature for their customers. In addition, some companies provide services that depend on access to unencrypted customer data. For example, some social networks encrypt data sent over the link between the user and the website, but process the data in the clear once it has been received.[175] Similarly, some cloud-storage services encrypt their customers' data, but unless their customers separately encrypt their data, these cloud providers maintain access to their own encryption keys.

Response to Argument 3: Allowing users to control their own keys increases security.

Reducing the number of entities that have the key to encrypted data reduces the number of potential attacks on the data.[176] In other words, there are fewer opportunities for user data to be stolen or leaked. The idea of users controlling their own keys is not new. Until cloud computing introduced a third party into the technical architecture, there was no technical reason to share encryption keys with anyone other than the parties communicating.[177] Indeed, many cloud-computing providers are starting to offer client-side encryption, which allows users to maintain control of the encryption keys just as they would in a non-cloud computing environment. For example, Google announced that the Google Cloud Compute Engine, its scalable cloud-based computing infrastructure, now allows customers to supply their own encryption keys.[178] Not only does this form of encryption allow customers to better manage risk for their data, but it also reduces the risk and liability of third parties holding that data. This will ultimately result in lower prices.

Of course, not all cloud-computing providers will adopt client-side encryption. For example, some may prefer to offer server-side encryption so that if the customer loses the key, access to the data can be recovered. Or a company's business model may depend on access to unencrypted data. But these decisions will vary from company to company.

Information security has drastically improved over the years to suit the needs and technologies of the time. Prohibiting companies from selling products and services that allow customers to maintain control of their encryption keys would turn back progress in information security, such as by limiting perfect forward secrecy. In addition, these limitations could make certain forms of technology, such as cloud computing, less viable for the private sector and limit IT-driven innovation.

Restricting innovation in information security would also have a negative impact on the security of the U.S. government. The Clinger Cohen Act of 1996 directs the federal government to acquire IT from the private sector.[179] As a result, the U.S. government, including the military, increasingly relies on commercial IT from the private sector for secure data storage and communications.[180] Therefore, any limitations on commercial innovation of IT security products will have an adverse effect on government information security.

Argument 4: Technologists have not tried to solve the problem.

In response the above critiques, some law enforcement officials have conceded that not allowing users to manage their own encryption keys may make consumers and businesses less secure. However, this has not stopped them from asking technologists to invent a method that allows lawful access by third-party actors while not introducing any vulnerabilities that could be exploited by bad actors. For example, Executive Assistant Director Hess and Director Comey have asked for "both government and industry to develop innovative solutions to secure networks and devices, yet still yield information needed to protect our society against threats and ensure public safety."[181] Director Comey expanded on this idea during a U.S. Senate hearing:

> "I hear lots of folks say it is too hard, can't be fixed. My response is, really? I think Silicon Valley is full of folks who stood in their garage and years ago were told, 'Your dreams are too hard to achieve. It is too hard.' Thank goodness they didn't listen. And they have built remarkable things that have changed our lives. Maybe it is too hard, but given the stakes—security on the Internet and public safety for the good folks of this country—we've got to give it a shot."[182]

This sentiment was echoed recently by former Secretary of State Hillary Clinton, who in the course of running a presidential campaign, has advocated for a "Manhattan-like Project" for dealing with the issue of encryption.[183] Secretary Clinton is not alone in these sentiments, as other presidential contenders Governor John Kasich and Donald Trump have hinted at similar measures to stop terrorists from exploiting encryption.[184] The theory goes that if enough technical experts are put in a room, they will find a way to create a system that allows third-party access to encrypted data without introducing vulnerabilities. The *Washington Post* editorial board echoed similar claims, writing "…with all their wizardry, perhaps Apple and Google could invent a kind of secure golden key they would retain and use only when a court has approved a search warrant."[185] Indeed, the *Washington Post* has continued to push for this approach, and has called for the National Academy of Sciences to study the issue further to with special focus on technical matters and to offer recommendations on how to give law enforcement access while maintaining protection against bad actors.[186] To this end, Representative Michael McCaul (R-TX) has announced a special congressional commission to find common ground between law enforcement, civil society advocates, and tech companies.[187]

Response to Argument 4: Encryption uses math, not magic.

While law enforcement may wish there was an alternative technical solution available, there is no technological solution to square this circle. Encryption is fundamentally math, and it cannot be bent or changed by gifted engineers or tech geniuses. The fact of the matter is, cryptographers have worked for decades to understand the problems, the tradeoffs, and the risks inherent with any system that builds in third-party access. Any proposal to allow a third-party access to encrypted data—whether through a "golden key," a "front door," Thor's hammer, or whatever someone wishes to call it—creates a new vulnerability.[188] There is simply no way to ensure that third-party access by a company or government actor is not also abused by adversaries.

While law enforcement may wish there was an alternative technical solution available, there is no technological solution to square this circle.

Argument 5: At a minimum, companies should help law enforcement officials hack into specific encrypted systems.

Recently, law enforcement officials have suggested that device makers should be required to make a special version of their software with disabled security features that could be installed on a suspect's device to make it easier for law enforcement to hack into it. This debate has circled around a specific case: The FBI is attempting to access the contents of an iPhone found in possession of one of the deceased San Bernardino terrorists, and it has been unable to do so for over two months.[189] In February 2016, a federal judge in California, responding to law enforcement's authority under the 200-year old All Writs Act, ordered Apple to install software on the device that would help federal investigators use brute force to access the phone.[190] In response, Apple has challenged this court order.[191]

The weakness that the FBI is trying to exploit is the phone's passcode, which only has 10,000 or 1 million possible answers depending on whether a user users a 4-digit or 6-digit code. With so few options, an adversary could use an automated brute-force attack to try every combination. To mitigate this vulnerability, Apple uses standard security techniques: It creates a delay after an incorrect guess before a new one can be made, and it allows users to permanently disable access if too many incorrect guesses are made.[192] In this case, the FBI has obtained an order requiring Apple to create a modified version of its operating system with these two security features disable and to install it on the device. This would allow the FBI to use brute force to figure out the passcode in seconds. The FBI's proposal would not work on newer iPhone operating systems, which have their own internal timer that cannot be changed with a software update.[193] Therefore, this is a very specific case, and Apple will not be able to comply with similar requests for its newer models.

Response to Argument 5: Companies should comply with lawful government requests to the extent they are able, but the government should not impose any design requirements on them.

Companies should be free to make the most secure products and services possible. The government should not be allowed to mandate that companies alter the design of the products and services they sell to facilitate government access to customer data. Congress has consistently avoided implementing technology mandates, even in legislation such as the USA Patriot Act, and it should continue to do so.[194] The government should also not be allowed to request that companies take actions to facilitate an investigation that would expose non-targeted users to new vulnerabilities. But if a company can comply with a lawful government request, it should. In addition, companies should not be restricted from making changes that make these requests impossible to fulfill, as such changes not only prevent government access, but also prevent third parties from hacking into devices.

While the Apple case is limited to a single phone, it would set a precedent that law enforcement could use in court orders to force companies to help law enforcement hack into specific devices and accounts in the future, including online services, connected cars, and smart-home devices. If this type of authority were abused by law enforcement, it could dissuade consumers from adopting these products. In particular, consumers might be reluctant to adopt smart-home technologies, like the Nest Camera or Amazon Echo, if law enforcement used their authority to conduct surveillance in the home using the cameras and microphones found in these types of consumer products. Furthermore, if users distrust the companies that make their devices, they may engage in bad security practices, such as disabling or delaying software updates, thereby leaving more devices unpatched and exposed to vulnerabilities.

However, if this type of investigatory authority is used only under limited circumstances and with strong judicial oversight, the impact on the average law-abiding consumer should be negligible. Thus, courts should grant law enforcement this authority for exceptional cases; in turn, law enforcement should use restraint in making these requests, and companies should comply when they are able. However, since these types of hacks still present a security weakness, the private sector should be free to develop more secure systems that do not have these vulnerabilities.

THE IMPACTS OF LIMITING ENCRYPTION

In addition to security impacts, mandating that all encryption systems provide extraordinary access will have several other impacts on the U.S. digital economy, including increased costs, decreased competitiveness, and diminished U.S. leadership.

Increased Costs for Consumers

Businesses can reduce risk by allowing customers to encrypt their own data. However, mandating key escrow systems not only drives up costs for the business associated with the new system, but also increases the risk associated with these systems. All of these increased costs are then passed on to consumers.

First, companies that are forced to operate key recovery systems will likely face increased operational costs, product design and engineering costs, government oversight costs, and user costs.[195] Operational costs would likely be the most immediate new costs of these systems, as businesses attempt to secure new vulnerable key recovery infrastructure from attacks. Companies may need to keep a copy of encrypted materials forever to satisfy possible future court orders, increasing electronic storage costs. These costs are hard to quantify because it is still unclear what entity would be responsible for ensuring that businesses maintain extraordinary access, how that policy would be enforced, and whether the government provides compensation to private-sector providers for the costs imposed. Second, by forcing businesses to retain access to customer data, law enforcement officials are also increasing the risk associated with these systems, and therefore the costs. This new system would add complexity and vulnerabilities that would force businesses to incur additional costs related to protecting their systems.

Lack of Trust Undermines U.S. Competitiveness

The U.S. government's failure to reform many of its intelligence community's surveillance programs has already damaged the competitiveness of the U.S. tech sector and cost it a portion of the global market share. Programs such as PRISM and Bullrun, the NSA's controversial programs that allow for warrantless access to private-user data on popular online services, and that undermine encryption standards, respectively, have fundamentally shaken international trust in U.S. tech companies and hurt U.S. business prospects.[196] Introduction of mandatory key escrow systems in U.S. products and services will exacerbate this problem, allowing foreign companies to convince their customers to keep data with domestic companies as a safer strategy than sending data abroad.

Several companies have come forward to describe how this loss of trust has damaged their ability to do business abroad. For example, the software-as-a-service company Birst has found that companies in Europe do not want their data hosted in North America due to concerns about U.S. spying.[197] In order to address these concerns, Birst was forced to partner with a European-based company to access European businesses. Outside the tech sector, other U.S. companies have reported that U.S. surveillance activities have caused them to lose major contracts to foreign competitors. For example, in December 2013, Boeing lost a contract to Saab AB to replace Brazil's aging fighter jets due to concerns over NSA activities, even though the airline had nothing to do with electronic surveillance.[198]

At the same time, foreign companies have made the U.S. digital surveillance policy a centerpiece of their own effective marketing strategy. Some European companies have begun to highlight where their digital services are hosted as an alternative to U.S. companies. German cloud companies like Hortnetsecurity bill themselves as "Cloud Services: Made in Germany," while French companies like Cloudwatt have joined the "Sovereign Cloud," a service advertised as resistant to NSA spying.[199] In addition, some countries, such as Germany, have voiced support for widespread adoption of encryption.[200] A mandatory key escrow system would make U.S. cloud providers less secure and less competitive, creating a new opportunity for eager foreign firms to gain market share.

This trend will be exacerbated if the U.S. government imposes any restrictions on commercial encryption. Foreign customers will not want to buy or use online services, hardware products, software products or any other information systems from U.S. companies that are designed expressly to give FBI or NSA access if they have more secure alternatives.

The U.S. Will Have Less Standing to Convince Other Nations to Avoid Policies That Undermine Encryption

Countries around the world, including U.S. allies, are considering a raft of new policies that could potentially weaken encryption standards or ban strong encryption. Countries such as China, India, and the United Arab Emirates either tightly control or have sought methods by which companies would be required to implement key escrow systems or otherwise create backdoors as a condition of market access.[201] If the United States continues to seek to ban end-to-end encryption or mandate key escrow, it will make it easier for some countries to push for reciprocal laws, introducing myriad vulnerabilities into the globally connected Internet.

It is not likely that U.S. actions one way or the other will be the deciding factor in what some nations, especially non-democratic ones, do with regard to encryption policy. For example over the last year and a half, China has considered several "counter-terrorism" laws that would effectively create key escrow systems in encryption products.[202] These laws would require tech companies that serve crucial sectors (e.g., banks) to sign a "voluntary" pledge that their products are "secure and controllable"—something that could be used to force companies to give third-party access to these systems. Seeing this law as in part a mercantilist tool to discriminate against foreign tech companies, President Obama pushed back against it, urging China to change the policy.[203] However, China's central government ignored the pressure from President Obama, citing efforts by both the United States and the United Kingdom to mandate similar key escrow systems in its justification for the law.[204] China eventually passed the law in July and started circulating the "secure and controllable" pledge to U.S. companies.[205] In February, 2016, the ambassadors of several nations warned China that these types of laws could harm both commerce and innovation.[206]

However, U.S. action may have more effect on our allies. In the United Kingdom, the Home Office—the government department that leads on crime policy and counter terrorism—sought to add a ban on strong encryption to its recently released online surveillance Investigatory Powers Bill, dubbed the Snoopers Charter.[207] Facing backlash from civil liberties groups, the U.K. government dropped several contentious proposals related to encryption before it released the draft.[208] But while the government officially backtracked, announcing that it would not seek backdoors in encrypted communications, the proposed draft legislation would have the opposite effect, forcing companies to include capabilities accessing communications if requested to do so.[209] Indeed, provisions in the bill can be construed to prevent companies from including end-to-end encryption in their products.[210]

Moreover, the policy choices one country makes can affect the security of others.[211] How secure would the United States be if China mandated the incorporation of a homegrown untested encryption algorithm into products and services for all firms outside the country that wish to do business with it? In this hypothetical, one country's weak standards could jeopardize the overall security of all Internet products and services. As another example, take India's business process outsourcing sector, which routinely exchanges sensitive data (e.g., health, employment, or financial data) with Europe and the United States.[212] If the Indian government mandated weakened encryption on all information within its borders, as it tried to do when the Department of Telecommunications proposed limiting Internet service providers to 40-bit encryption keys, this data could be easily compromised.[213]

RECOMMENDATIONS

The ability of consumers and businesses to protect sensitive information has allowed the digital economy to flourish. Rather than place barriers on encryption, the U.S. government should advocate for better cybersecurity practices both domestically and abroad, in part by encouraging continued innovation in encryption. Congress and the administration can do so by replenishing trust and strengthening data security at home, providing law enforcement with new tools to uphold the law, and projecting the United States' firm commitment to data security to the world.

Strengthen Trust and Security at Home

It is imperative for the United States to reestablish trust in its government institutions and the U.S. private sector. To that end, there are a number of policy changes the U.S. government can make.

First, the U.S. Congress should revoke the statutory mandate for NIST to work with other agencies to establish encryption standards.[214] The U.S. government should restore trust in NIST-backed encryption standards by being forthcoming and transparent about the intelligence community's involvement in standards development. Reliable technical standards are crucial in a world dependent on secure electronic communications and commerce, critical infrastructure, as well as personal privacy. The NSA has engaged in systematic efforts to weaken or disrupt encryption standards, often surreptitiously. In addition, the NSA should be transparent about its work to weaken U.S. security products. The NSA operates the "Commercial Solutions Center," which invites the creators of commercial hardware and software encryption products to present their products to the agency with the stated goal of improving overall security through public-private partnerships.[215] However, the *New York Times* cites a top-secret document suggesting that the NSA hacking division uses this opportunity to "leverage sensitive, cooperative relationships with specific industry partners" to add weaknesses into presented security products.[216]

Second, the U.S. Congress should pass legislation, similar to the Secure Data Act introduced by Senator Ron Wyden (D-OR) in 2015, banning the government from installing backdoors and offering full support for encryption.[217] Lawmakers should expand these legislative efforts to ban government mandates for key escrow systems, such as those where businesses are required to hold a copy of the encryption keys to customer products. This law should ensure that the U.S. government does not interfere with technological or design decisions that companies make about the products they sell. This legislation should also preempt all state efforts to create similar measures, as proposed in the Ensuring National Constitutional Rights of Your Private Telecommunications (ENCRYPT) Act of 2016, introduced by Representatives Blake Farenthold (R-TX) and Ted Lieu (D-CA).[218] Preemption would help establish a uniform system that encourages the use of encryption technologies. In the short term, President Obama, or his successor, should sign an executive order for the federal government formalizing this policy as well. This legislation should draw a clear line in the sand and declare that the policy of the U.S. government is to strengthen, not weaken information security.

Third, when U.S. government agencies discover security flaws, including in cryptographic protocols, they should report 100 percent of them to companies in a timely and responsible manner so companies can fix these flaws. To date, the NSA's website states that the agency reveals the most serious security flaws it finds about 91 percent of the time.[219] By the agency's admission, the other 9 percent are not disclosed because developers either patched them prior to disclosure or due to "national security reasons." However, when U.S. government agencies discover vulnerabilities in software or hardware products, they should responsibly notify these companies in a timely manner every time to fix the vulnerabilities. The best way to protect U.S. citizens and businesses from digital threats is to promote strong cybersecurity practices in the private sector.

Achieving a fair balance of interests between citizens and the state requires permitting law enforcement—under lawful court order—to compel someone to turn over their password or encryption key.

Provide Law Enforcement with Additional Tools

It is important to recognize that law enforcement's capacity to solve some cases may be diminished due to the increasing adoption of encryption. As a result, law enforcement needs new legal and educational tools to overcome this challenge.

First, the U.S. Congress should study whether legislation can help U.S. courts better balance the interests of the individual and the state by allowing law enforcement to compel the production of decrypted data.[220] The Fifth Amendment attempts to create a fair government-individual balance by weighing the privileges of the individual with the needs of society.[221] However, encryption offers a unique and significant interest for the state in compelling production of decrypted information, as encrypted information is often impregnable without the key. Achieving a fair balance of interests between citizens and the state requires permitting law enforcement—under lawful court order—to compel someone to turn over their password or encryption key if law enforcement can prove a convincing interest in acquiring that information. To achieve this, the U.S. Congress could pass a law codifying these powers, and U.S. courts can uphold this approach to help provide balance to the system.

Under this approach, a defendant could be held in contempt of court for refusing to comply with a lawful court order to turn over an encryption key. If law enforcement brought a case whereby it could not prove a compelling need for encrypted information, the judge could deny the court order. This would add a tool to law enforcement toolboxes, allowing them to circumvent encryption barriers and solve cases without weakening encryption standards. To be sure, this method will not address all of the government's needs, such as when it desires to secretly obtain information without alerting a suspect. In addition, the key may occasionally be obtained through reasonable investigative methods that do not deal with Fifth Amendment protections, such as through the use of a keylogger or surveillance video.

Second, the U.S. Congress should offer additional resources to state and local law enforcement for cyberforensics and to incentivize resource sharing. Despite the rapid evolution of encryption and the increased prevalence of cybercrime, state and local law enforcement has been ill-equipped to investigate and prosecute a rash of new criminal activity. To help bridge this gap, there have been a number of federal efforts to strengthen state and local cyberforensics expertise. For example, the Secret Service's National Computer Forensics Institute trains state and local law enforcement officers, prosecutors, and judges across the country in cyber investigative techniques.[222] Similarly, the FBI offers limited cybercrime assistance through cyber task forces.[223] However, these efforts are not enough. To respond to state and local law enforcement needs, the U.S. Congress should offer states funding to pursue better cyberforensics and encourage greater resource and intelligence sharing between different levels of law enforcement. For example, Congress could support the creation of a dedicated national service to provide state and local law enforcement greater technical assistance during investigations.

Establish Clear Rules for Government Hacking

Congress should establish clear and well-defined rules for how and when the government can engage in hacking. Current rules governing this issue occupy a legal grey area.[224] And there are complicated rules that make it difficult for the FBI to obtain a warrant to hack into a system because of questions of jurisdiction.[225] Congress should have an open debate about these issues and establish clear and consistent rules for how and when law enforcement can hack into systems, including any assistance the private sector should provide and transparency requirements. This will ensure that law enforcement has the appropriate authority to pursue investigations while also ensuring that Fourth Amendment rights are protected and the impact on companies is minimized.

Pursue a Pro-Cybersecurity Foreign Policy Agenda

The United States should be a global champion for strong information security by creating a broader strategy for improving cybersecurity around the world.

First, the U.S. government should create a pro-cybersecurity foreign policy strategy that seeks to push back against countries that try to weaken encryption standards for anti-competitive reasons. In addition, the U.S. government should push its allies to reject policies that undermine cybersecurity within their borders, as with an increasingly networked economy this weakens security for everyone. By leading on international issues of information security, the United States can help improve the security of the global Internet economy.

Second, the U.S. government should push back against weakened encryption standards abroad by completing trade agreements that work to eliminate them. U.S. negotiators should ensure that trade agreements, including the Trans-Atlantic Trade and Investment Partnership (T-TIP), and the Trade in Services Agreement (TISA), are strongly in favor of robust information security practices. The United States should build an alliance against bad actors, forcing protectionist countries to the sidelines of the global trade arena if they continue to enact anti-competitive rules or rules that undermine information technology products and services. Furthermore, as the U.S. Congress weighs future trade promotion authority, it should direct U.S. negotiators to include prohibitions against countries with weakened encryption standards in all future U.S. trade agreements.

Finally, the U.S. government should work with its allies to establish international legal standards for government access to data, building on existing efforts such as the Budapest Convention on Cybercrime.[226] The global nature of the Internet makes access to information by law enforcement difficult to enforce and legal jurisdictions hard to define. This would especially be the case with extraordinary access, as criminals and citizens could simply buy products from countries that do not cooperate with laws that mandate a set of keys for law enforcement. Therefore, the United States should work with its trading partners to develop a "Geneva Convention on the Status of Data."[227] This would create a multilateral agreement that would establish international rules for transparency, settle questions of jurisdiction, engender cooperation for better coordination of international law enforcement requests, and limit unnecessary access by governments to citizens of other countries. Only by working to establish a global pact on these issues can countries that have previously engaged in mass cyberespionage assure the international community that countries can hold each other accountable in the future, and that law enforcement can work together to solve multijurisdictional crimes.

CONCLUSION

U.S. efforts to mandate extraordinary access to encryption products and services will reduce progress in information security systems and serve only to open foreign markets for foreign competitors, as they did in the first crypto wars. The policy of the U.S. government should not be to pick winners and losers by mandating specific technologies. Doing so will actively halt innovation in information security, creating a digital world that is less secure overall. Instead, the United States should stand athwart any attempts to denigrate cybersecurity and should champion strong encryption by promoting a broader strategy for improving cybersecurity around the world.

ENDNOTES

1. James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *Federal Bureau of Investigations*, October 16, 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
2. Trevor Tim, "The FBI used to recommend encryption. Now they want to ban it," *The Guardian*, March 28, 2015; Liz Gannes, "Obama: 'There's No Scenario in Which We Don't Want Really Strong Encryption'," *Recode*, accessed January 4, 2016, http://recode.net/2015/02/13/obama-theres-no-scenario-in-which-we-dont-want-really-strong-encryption/.
3. These attempts include banning the export of certain types of encryption, undermining encryption standards, building back doors software and hardware, asking the private sector to develop key escrow or intercept capabilities, and developing capabilities to use brute-force to decrypt encrypted data. See 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," *Berkeley Roundtable on the International Economy*, February 21, 2003, http://escholarship.org/uc/item/89r4j908; Larry Greenemeier, "NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard," *Scientific American*, September 18, 2013, http://www.scientificamerican.com/article/nsa-nist-encryption-scandal/; Evan Perez and Shimon Prokupecz, "First on CNN: Newly discovered hack has U.S. fearing foreign infiltration," *CNN*, December 19, 2015, http://www.cnn.com/2015/12/18/politics/juniper-networks-us-government-security-hack/; "Discovering IT problems, Developing Solutions, Sharing Expertise," *U.S. National Security Agency*, October 30, 2015, https://www.nsa.gov/public_info/news_information/2015/ncsam/discovering_solving_sharing_it_solutions.shtml.
4. Steven Levy, "Battle of the Clipper Chip," *New York Times*, June 12, 1994, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.
5. Larry Greenemeier, "NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard;" Joseph Menn, "NSA says how often, not when, it discloses software flaws," *Reuters*, March 30, 2015, http://www.reuters.com/article/us-cybersecurity-nsa-flaws-insight-idUSKCN0SV2XQ20151107#QZF5OuhmEg2KCeA5.97.
6. Daniel Castro and Alan McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness," *Information Technology and Innovation Foundation*, June 2015, http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.110906501.1240521073.1404749065.
7. "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," *U.S. Senate Committee on the Judiciary*, video, 1:41, July 8, 2015, http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy.
8. Ellen Nakashima, "Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks," *Washington Post*, February 17, 2016, https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html.
9 For example, see Mike McConnell, Michael Chertoff and William Lynn, "Why the fear over ubiquitous data encryption is overblown," *Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.
10. For examples of heated rhetoric please see Amie Stepanovich, "Opinion: Britain can't pwn the world," *The Christian Science Monitor*, January 12, 2016, http://www.csmonitor.com/World/Passcode/2016/0112/Opinion-Britain-can-t-pwn-the-world; "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," *U.S. Senate Committee on the Judiciary*, July 8, 2015, http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy.
11. Karla de Leeuw and Jan Bergstra, *The History of Information Security: A Comprehensive Handbook* (Elsevier: Oxford, 2007), 613.
12. David Banisar, "Stopping Science: The Case of Cryptography," *Health Matrix: Journal of Law-Medicine*, Vol. 9, February 1999, 253, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1806222.
13. 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."

14. “Cryptography for a Connected World,” *IBM*, accessed February 4, 2016, http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/cryptography/.
15. Arthur Sorkin, “Lucifer, A Cryptographic Algorithm,” *Lawrence Livermore National Laboratory*, April 1983, http://www.fuseki.com/lucifer.pdf.
16. “Cryptography for a Connected World,” *IBM.*
17. Top secret information was secured with other algorithms that were not public. Stephen Pincock, *Codebreaker: The History of Codes and Ciphers, From the Ancient Pharaohs to Quantum Cryptography* (New York: Walker & Company, 2006), 141.
18. “Data Encryption Standard,” *National Institute of Standards and Technology*, accessed February 16, 2016, http://nvlpubs.nist.gov/nistpubs/sp958-lide/250-253.pdf.
19. Ibid.
20. William Jackson, “NSA reveals its secret: No backdoor in encryption standard,” *GCN*, February 16, 2011, https://gcn.com/articles/2011/02/16/rsa-11-nsa--no-des-backdoor.aspx.
21. David Banisar, “Stopping Science: The Case of Cryptography.”
22. 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.”
23. Ibid.
24. Charles Sykes, *The End of Privacy* (New York: St. Martin’s Press, 1999), 173.
25. 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.”
26. 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.
27. 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.”
28. Steven Levy, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*. (Viking Penguin Books: New York, 2001).
29. “Record set in cracking 56-bit crypto,” *CNET*, January 2, 2002, http://www.cnet.com/news/record-set-in-cracking-56-bit-crypto/.
30. James Nechvatal et al, “Report on the Development of the Advanced Encryption Standard,” *National Institute of Standards and Technology,* October 2, 2000, http://csrc.nist.gov/archive/aes/.
31. “Cryptography Today,” *National Security Agency*, accessed February 2, 2016, https://www.nsa.gov/ia/programs/suiteb_cryptography/.
32. Public key encryption dated back to the 1970s, but it was not until the 1990s that these protocols were secure enough to use in the real world. For e.g. see RSA and Diffie-Hellman. “A Brief history: The Origins of Public-Key Cryptography and ECC,” *Certicom*, accessed January 4, 2016, https://www.certicom.com/index.php/a-brief-history.
33. Whitefield Diffie and Martin Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory*, Vol. 22, No. 6, November 1976, https://www-ee.stanford.edu/~hellman/publications/24.pdf; Ronald Rivest, Adi Shamir, and Leonard Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Massachusetts Institute of Technology*, accessed February 16, 2016, https://people.csail.mit.edu/rivest/Rsapaper.pdf.
34. “Secure Sockets Layer (SSL),” *TechTarget*, accessed February 16, 2016, http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL.
35. Craig Timberg, “A Flaw in Design,” *Washington Post*, May 30, 2015, http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.
36. Ryan Hagemann and Josh Hampson, “Encryption, Trust, and the Online Economy,” *Niskanen Center*, November 9, 2015, https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits_FINAL.pdf.
37. “Global Internet Phenomena Spotlight,” *Sandvine*, April 8, 2015, https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf.
38. Valeria Caproni, “Going Dark: Lawful Electronic Surveillance in the Face of New Technologies,” *Federal Bureau of Investigations*, February 17, 2011, https://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies.

39. 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.”
40. Comprehensive Counter-Terrorism Act of 1991, S. 266, 102nd Cong. (1991), accessed January 4, 2016, https://www.congress.gov/bill/102nd-congress/senate-bill/266.
41. 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.
42. Steven Levy, “Battle of the Clipper Chip.”
43. “Questions and Answers About the Clinton Administration’s Encryption Policy,” *Electronic Privacy Information Center*, February 4, 1994, https://epic.org/crypto/clipper/clipper_q_and_a_feb_94.html.
44. 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.
45. Ronald Stay, “Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann,” *Georgia State University Law Review*, Vol. 13, Issue 2, February 1997, http://readingroom.law.gsu.edu/cgi/viewcontent.cgi?article=2264&context=gsulr.
46. Ira Rubinstein and Michael Hintze, “Export Controls on Encryption Software,” *Practising Law Institute*, December 2000, http://encryption_policies.tripod.com/us/rubinstein_1200_software.htm.
47. Ibid.
48. 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.”
49. To be precise, the Clinton Administration declared that encryption key length would no longer be a major factor in determining the exportability of cryptographic products. Groups such as Americans for Computer Privacy (ACP), helped push for this goal by promoting pro-encryption legislation. Whitfield Diffie and Susan Landau, “The Export of Cryptography in the 20th Century and the 21st,” *Handbook of the History of Information Security*, April 19, 2005, http://privacyink.org/pdf/export_control.pdf; Steven Levy, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (Viking Penguin Books: New York, 2001).
50. R. U. Sirius, “Cypherpunk rising: WikiLeaks, encryption, and the coming surveillance dystopia,” *The Verge*, March 7, 2013, http://www.theverge.com/2013/3/7/4036040/cypherpunks-julian-assange-wikileaks-encryption-surveillance-dystopia.
51. Philip Zimmerman, “Why I Wrote PGP,” *PhilZimmermann.com,* 1991, updated in 1999, https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.
52. Derek Atkins, William Stallings and Philip Zimmermann, “PGP Message Exchange Formats,” *Network Working Group*, August 1996, https://www.ietf.org/rfc/rfc1991.txt.
53. Philip Dubois, “Significant Moments in PGP's History: Zimmermann Case Dropped,” *PhilZimmermann.com*, January 12, 1996, https://www.philzimmermann.com/EN/news/PRZ_case_dropped.html.
54. Bernstein v. United States Department of Justice, No. 97-16686, (9th Cir. May 6, 1999), http://caselaw.findlaw.com/us-9th-circuit/1317290.html.
55. 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.”
56. “Special White House Briefing Encryption Technology,” *Electronic Frontier Foundation*, accessed January 26, 2016, https://w2.eff.org/Privacy/Crypto_export/1999_export_policy/19990916_wh_briefing_transcript.html.
57. Arif Mohamed, “A history of cloud computing,” *Computer Weekly*, accessed January 4, 2016, http://www.computerweekly.com/feature/A-history-of-cloud-computing.
58. Ibid.
59. “Philips,” *Salesforce*, accessed February 17, 2016, https://www.salesforce.com/customers/stories/philips.jsp.
60. Ben Rossi, “Catastrophe in the cloud: What the AWS hacks mean for cloud providers,” *Information Age*, August 27, 2014, http://www.information-age.com/technology/cloud-and-virtualisation/123458406/catastrophe-cloud-what-aws-hacks-mean-cloud-providers; Paul Roberts, “Five Devastating Hacks that Predate Sony,” *Digital Guardian*, September 28, 2015, https://digitalguardian.com/blog/five-devastating-hacks-predate-sony.
61. Eric Blattberg, “Apple starts encrypting all iCloud emails,” *Venture Beat*, July 15, 2014, http://venturebeat.com/2014/07/15/apple-starts-encrypting-all-icloud-emails/.

62. Ken Beer and Ryan Holland, “Encrypting Data At Rest,” *Amazon Web Services*, November 2014, https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf.
63. Daisuke Wakabayashi, “Tim Cook Says Apple to Add Security Alerts for iCloud Users,” *Wall Street Journal*, September 5, 2014, http://www.wsj.com/articles/tim-cook-says-apple-to-add-security-alerts-for-icloud-users-1409880977.
64. “A Brief History of Malware,” *Trend Micro*, accessed January 9 ,2016, https://countermeasures.trendmicro.eu/wp-content/uploads/2012/02/History-of-Mobile-Malware.pdf.
65. “Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP),” *Federal Communication Commission*, December 4, 2014, http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf.
66. “The Symantec Smartphone honey Stick Project,” *Symantec*, 2012, http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf.
67. Ibid.
68. Craig Timberg, “Newest Androids will join iPhones in offering default encryption, blocking police,” *Washington Post*, September 18, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/; Craig Timberg, “Apple will no longer unlock most iPhones, iPads for police, even with search warrants,” *Washington Post*, September 18, 2014, https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html.
69. Andy Boxall, “Apple says it can’t break into new iPhones, even if the government tells it to,” *Digital Trends*, October 21, 2015, http://www.digitaltrends.com/apple/apple-justice-department-encrypted-data-news/.
70. This is not offered by default. “A sweet Lollipop, with a kevlar wrapping: New security features in Android 5.0,” *Android Official Blog*, October 28, 2014, http://officialandroid.blogspot.com/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html.
71. When a company encrypts storage on a device, the passcode that the user enters is usually not also the encryption key. Instead, a random key encrypts the device and the user’s passcode encrypts the random key.
72. For example, see, “Use a passcode with your iPhone, iPad, or iPod touch,” *Apple*, accessed February 29, 2016, https://support.apple.com/en-us/HT204060.
73. Daniel Castro and Jordan Misra, “The Internet of Things,” *Center for Data Innovation*, November 2013, http://www2.datainnovation.org/2013-internet-of-things.pdf.
74. Vaughan Emery, “End-to-end encryption is key for securing the Internet of Things,” *HelpNetSecurity*, September 7, 2015, https://www.helpnetsecurity.com/2015/09/07/end-to-end-encryption-is-key-for-securing-the-internet-of-things/; Curt Schwaderer, “Protecting the IoT and connected automotive systems against purpose-built attacks,” *Embedded Computing Design*, February 27, 2016, http://embedded-computing.com/articles/protecting-iot-connected-against-purpose-built-attacks/.
75. Gartner, “Gartner Says 6.4 Billion Connected ‘Things’ Will Be in Use in 2016, Up 30 Percent From 2015,” news release, November 10, 2015, https://www.gartner.com/newsroom/id/3165317.
76. James Manyika et al., “Unlocking the potential of the Internet of Things,” *McKinsey & Company*, June 2015, http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.
77. James Clapper, “DNI Clapper Opening Statement on the World Threat Assessment,” *Office of the Director of National Intelligence*,” February 9, 2016, http://www.dni.gov/index.php/newsroom/testimonies.
78. James Comey, “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” *Federal Bureau of Investigations*, October 16, 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
79. “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy,” *U.S. Senate Committee on the Judiciary*, July 8, 2015, http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy; “Hearings,” *U.S. Senate Select*

Committee on Intelligence, July 8, 2015, http://www.intelligence.senate.gov/hearings/counterterrorism-counterintelligence-and-challenges-going-dark.

80. This would be the effect of the following proposed language, "Any smartphone that is manufactured on or after XX, and sold or leased in New York, shall be capable of being decrypted and unlocked by its manufacturer or its operating system provider." See, "Report of the Manhattan District Attorney's Office On Smartphone Encryption and Public Safety," *District Attorney of New York County*, November 2015, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.
81. Adam Bienkov, "David Cameron: Twitter and Facebook privacy is unsustainable," *Politics.co.uk*, June 30, 2015, http://www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable.
82. Rob Price, "David Cameron Wants To Ban Encryption," *Business Insider*, January 12, 2015, http://www.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1.
83. Rob Price, "European police chief: Encryption is the 'biggest problem' in tackling terrorism," *Business Insider*, March 30, 2015, http://www.businessinsider.com/europol-wainright-encryption-biggest-problem-tackling-terrorism-apple-google-2015-3 .
84. Ronald Hosko, "Apple and Google's new encryption rules will make law enforcement's job much harder," *Washington Post*, September 23, 2014, https://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/.
85. Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity By Requiring Government Access To All Data and Communications," *Schneier on Security*, July 7, 2015, https://www.schneier.com/cryptography/paperfiles/paper-keys-under-doormats-CSAIL.pdf.
86. David Kravets, "Apple CEO Tim Cook blasts encryption backdoors," *Ars Technica*, October 20, 2015, http://arstechnica.com/tech-policy/2015/10/apple-ceo-tim-cook-blasts-encryption-backdoors/.
87. Mike McConnell, Michael Chertoff and William Lynn, "Why the fear over ubiquitous data encryption is overblown," *Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.
88. Jenna McLaughlin, "NSA Chief Stakes Out Pro-Encryption Position, in Contrast to FBI," *The Intercept*, January 21, 2016, https://theintercept.com/2016/01/21/nsa-chief-stakes-out-pro-encryption-position-in-contrast-to-fbi/; Ellen Nakashima and Barton Gellman, "As encryption spreads, U.S. grapples with clash between privacy, security," *Washington Post*, April 10, 2015, https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.
89. "An Open Letter to the Leaders of the World's Governments Signed by Organizations, Companies, and Individuals," *Secure the Internet*, accessed January 5, 2015, https://www.securetheinternet.org/.
90. *Access et al.,* "Letter to President Barack Obama," *New America.*, May 19, 2015, https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf.
91. Lisa Lambert and Jeff Mason, "Obama backs away from law to access encrypted information," *Reuters*, October 10, 2015, http://www.reuters.com/article/2015/10/10/us-usa-cybersecurity-legislation-idUSKCN0S40VN20151010#2oXbrfFQ3mltMlWX.97.
92. "We the People: Publically affirm your support for strong encryption," *The White House*, September 29, 2015, https://petitions.whitehouse.gov/petition/publicly-affirm-your-support-strong-encryption.
93. Rainey Reitman, "EFF, Access Now, and the White House Sat Down to Talk About Encryption: The Details," *Electronic Frontier Foundation*, December 16, 2015, https://www.eff.org/deeplinks/2015/12/eff-access-now-and-white-house-sat-down-talk-about-encryption-details.
94. Eric Geller, "Global coalition demands that world leaders support strong encryption," *The Daily Dot*, January 11, 2016, http://www.dailydot.com/politics/encryption-coalition-security-for-all-open-letter/.
95. Liam Tung, "Encryption backdoors by law? France says 'non'," *ZDNet*, January 18, 2016, http://www.zdnet.com/article/encryption-backdoors-by-law-france-says-non/; Robert Hackett, "Dutch Government Backs Uncrackable Encryption," *Fortune*, January 5, 2016, http://fortune.com/2016/01/05/dutch-government-encryption-no-backdoors/.
96. Robert Hannigan, "The web is a terrorist's command-and-control network of choice," *Financial Times*, November 3, 2014, http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3pmQuHztI.

97. Ashley Carman, “The U.S. government doesn’t know what technology to blame for the Paris attacks,” *The Verge*, November 18, 2015, http://www.theverge.com/2015/11/18/9755582/paris-attacks-cause-investigation-cia-fcc-encryption-internet.

98. Albert Gidari, “CALEA Limits the All Writs Act and Protects the Security of Apple’s Phones,” *The Center for Internet and Society*, February 19, 2016, https://cyberlaw.stanford.edu/blog/2016/02/calea-limits-all-writs-act-and-protects-security-apples-phones.

99. Cory Bennett, “Feinstein vows to offer bill to pierce encryption,” *The Hill*, December 9, 2015, http://thehill.com/policy/cybersecurity/262658-feinstein-vows-to-offer-encryption-piercing-bill.

100. John McCain, “Silicon Valley Should Join the War on Terrorism,” *BloombergView*, February 5, 2016, http://www.bloombergview.com/articles/2016-02-05/silicon-valley-should-join-the-war-on-terrorism.

101. National Commission on Security and Technology Challenges, H.R. 4651, 114th Cong. (2016), https://assets.documentcloud.org/documents/2724063/Commission-Xml-1.pdf.

102. Cyrus Farivar, “Yet another bill seeks to weaken encryption-by-default on smartphones,” *Ars Technica*, January 21, 2016, http://arstechnica.com/tech-policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones/.

103. Andrea Castillo, “Going Dark? Federal Wiretap Data Show Scant Encryption Problems,” *Mercatus Center*, February 26, 2016, http://mercatus.org/publication/going-dark-federal-wiretap-data-show-scant-encryption-problems.

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

105. Jenna McLaughlin, “NSA Is Mysteriously Absent From FBI-Apple Fight,” *The Intercept*, March 3, 2016, https://theintercept.com/2016/03/03/nsa-is-mysteriously-absent-from-fbi-apple-fight/.

106. “Two Gulf states to ban some Blackberry functions,” *BBC*, August 1, 2010, http://www.bbc.com/news/world-middle-east-10830485.

107. Josh Halliday and Saeed Shah, “Pakistan to ban encryption software,” *The Guardian,* August 30, 2011, http://www.theguardian.com/world/2011/aug/30/pakistan-bans-encryption-software.

108. 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.”

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

110. Soon after the algorithm was selected, security researchers discovered the vulnerability. Companies that used the algorithm would have been subject to attacks from the known vulnerability. Berry Schoemakers and Andrey Sidorenko, “Cryptoanalysis of the Dual Elliptic Curve Pseudorandom Generator,” *Pro Publica*, May 29, 2006, http://www.propublica.org/documents/item/786216-cryptanalysis-of-the-dual-elliptic-curve; Dan Schumow and Niels Furguson, “On the Possibility of a Back Door in the NIST SP800-90 Duel Ec Prng,” *Microsoft*, Pro Publica, accessed November 16, 2015, http://www.propublica.org/documents/item/786216-cryptanalysis-of-the-dual-elliptic-curve.

111. “NIST Initiating Review of Cryptographic Standards Development Process,” *National Institute of Standards and Technology,* January 23, 2014*,* http://csrc.nist.gov/groups/ST/crypto-review/index.html. “NIST Solicits Comments On Its Revised Cryptographic Standards and Guidelines Development Process,” *National Institute of Standards and Technology*, accessed March 8, 2016, http://csrc.nist.gov/groups/ST/crypto-review/process.html.

112. Bruce Schneier, “Did NSA Put A Secret Backdoor in New Encryption Standard,” *Wired*, November 15, 2007, http://www.wired.com/2007/11/securitymatters-1115/.

113. Sean Gallagher, “Photos of an NSA ‘upgrade’ factory show Cisco router getting implant,” *Ars Technica*, May 14, 2014, http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/.

114. Kim Zetter, Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA,” *Wired*, December 22, 2015, http://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/.

115. Emily Price, “Juniper Networks security flaw may have exposed US government data,” *The Guardian*, December 22, 2015, http://www.theguardian.com/technology/2015/dec/22/juniper-networks-flaw-vpn-government-data.

116. Ralf-Phillip Weinmann, "Some Analysis of the Backdoored Backdoor," *rpw*, accessed February 5, 2016, http://rpw.sh/blog/2015/12/21/the-backdoored-backdoor/.
117. Kate Knibbs, "The FBI has Its Own Secret Brand of Malware," *Gizmodo*, April 02, 2015, http://gizmodo.com/the-fbi-has-its-own-secret-brand-of-malware-1694821520; Kevin Poulsen, "The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users," *Wired*, December 16, 2014, http://www.wired.com/2014/12/fbi-metasploit-tor/.
118. Kevin Poulsen, "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats," *Wired*, September 18, 2007, http://www.wired.com/2007/07/fbi-spyware/.
119. Declan McCullagh, "Feds use Keylogger to thwart PGP, Hushmail," *CNET*, July 20, 2007, http://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail/.
120. "Gemalto presents the findings of its investigations into the alleged hacking of SIM card encryption keys by Britain's Government Communications Headquarters (GCHQ) and the U.S. National Security Agency (NSA)," *Gemalto*, February 25, 2015, http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx; Jeremy Scahill and Josh Begley, "The Great Sim Heist," *The Intercept*, February 19, 2015, https://theintercept.com/2015/02/19/great-sim-heist/.
121. "IMSIs Identified with Ki Data for network Providers Jan10-Mar10 Trial," *The Intercept*, February 19, 2015, https://theintercept.com/document/2015/02/19/imsis-identified-ki-data-network-providers-jan10-mar10-trial/.
122. Matthew Green, "How do we build encryption backdoors?" *Cryptographic Engineering*, April 16, 2015, http://blog.cryptographyengineering.com/2015/04/how-do-we-build-encryption-backdors.html.
123. "Read the Obama administration's draft paper on technical options for the encryption debate," *Washington Post*, accessed January 6, 2015, http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/; Cyrus Farivar, "Judge: Apple must help FBI unlock San Bernardino shooter's iPhone," *Ars Technica*, February 16, 2016, http://arstechnica.com/tech-policy/2016/02/judge-apple-must-help-fbi-unlock-san-bernardino-shooters-iphone/.
124. "Read the Obama administration's draft paper on technical options for the encryption debate," *Washington Post*, accessed January 6, 2015, http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/.
125. Ellen Nakashima and Barton Gellman, "As encryption spreads, U.S. grapples with clash between privacy, security," *Washington Post*, April 10, 2015, https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.
126. Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity By Requiring Government Access To All Data and Communications," *Schneier on Security*, July 7, 2015, https://www.schneier.com/cryptography/paperfiles/paper-keys-under-doormats-CSAIL.pdf.
127. Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity By Requiring Government Access To All Data and Communications."
128. Sandvine predicts that by the end of 2016, 65-70 percent of Internet traffic will be encrypted in most markets. Given that 33 gigabytes of information are exchanged on the Internet every second, there will be a substantial amount of encrypted material exchanged every moment. See "Global Internet Phenomena Spotlight," *Sandvine; "*One Second," *Internet Live Stats*, January 17, 2016, http://www.internetlivestats.com/one-second/.
129. Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum*, June 29, 2007, http://spectrum.ieee.org/telecom/security/the-athens-affair.
130. Tom Cross, "Exploring Lawful Intercept to Wiretap the Internet," *Black Hat*, 2010, https://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-LawfulI-Intercept-wp.pdf.
131. Jack Moore, "The Year of the Breach: 10 Federal Agency Data Breaches in 2014," *NextGov*, December 30, 2014, http://www.nextgov.com/cybersecurity/2014/12/year-breach-10-federal-agency-data-breaches-2014/102066/; Jeff Pegues, "Private Emails of CIA Director, DHS Secretary Hacked," *CBS*, October 29, 2015, http://www.cbsnews.com/news/cia-director-and-dhs-secretary-emails-hacked/.
132. Robert Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (Maryland: Sheridan Group, 2000), 160-180.

133. Law enforcement officials can compel a person to turn over encrypted information in certain circumstances if the existence of evidence on a device is a foregone conclusion and thus does not violate their Fifth Amendment rights. See, People v. Havrish, 8 N.Y. 3d 389, 395 (N.Y. 2007); In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1346 (11th Cir. 2012); In re Boucher, 2009 WL 424718 (D. Vt. Feb. 19, 2009); In re Fricosu, 841 F. Supp.2d 1232, 1237 (D. Colo. 2012).

134. James Comey, "Encryption Tightrope: Balancing Americans' Security and Privacy," *Federal Bureau of Investigation*, March 1, 2016, https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy; "House Judiciary Committee to Hold Hearing on Encryption," *U.S. House of Representatives Judiciary Committee*, video, February 25, 2016, http://judiciary.house.gov/index.cfm/press-releases?ContentRecord_id=3857071F-15C2-4F9E-B7C8-319B1DB2E132.

135. James Comey, "Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee Washington, D.C," *Federal Bureau of Investigations*, July 8, 2015, https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

136. These laws include title III of the Omnibus Crime Control and Safe Streets Act of 1968 (often referred to as Title III or the Wiretap Act), the Foreign Intelligence Surveillance Act of 1978 (FISA), or the Communications Assistance for Law Enforcement Act (CALEA). The Electronic Communications Privacy Act amended Title III.

137. U.S. Const. amend. V.

138. In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, (11th Circ. March 25, 2011)

139. This is because courts have applied the testimonial framework of strongbox keys versus safe combinations to unlocking passwords and encrypted information. The Supreme Court said in *Doe v. United States* that being forced to surrender a key to a strongbox is not testimonial, whereas compelled surrender of a safe combination is. This is ostensibly because strongbox keys exist in the physical world and a key can open them, while a safe combination exists is someone's mind, and being compelled to give it up would equate to creating evidence against that person (thus violating the privilege against self-incrimination). The courts have treated physical keys (e.g., a fingerprint) like the former, and passwords like the latter. See, Doe v. United States, 487 U.S. 201, (1988); Dan Terzian, "The Fifth Amendment, Encryption, and the Forgotten State Interest," *UCLA Law Review*, Disc. 298, 300-312, 2014, http://www.uclalawreview.org/pdf/discourse/61-19.pdf.

140. James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?"

141. "Smartphone Encryption and the Impact on Law Enforcement," *New York County District Attorney's Office*, presentation, accessed February 17, 2016, http://manhattanda.org/sites/default/files/Smartphone%20Encryption%20and%20the%20Impact%20on%20Law%20Enforcement%20v8.pdf.

142. Mark Rush, "Corporate Responses to Investigative Requests by the Federal Government," *K&L Gates*, 2014, http://www.klgates.com/files/Publication/0fffa665-105a-4792-8f9f-e70e4d1d1c77/Presentation/PublicationAttachment/9c0a79cc-6fa8-4013-a543-56097132ed9d/orporate_Responses_white_paper_for_Mark_Rush.pdf.

143. Cyrus Vance, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy." *Manhattan District Attorney*, July 8, 2015, http://www.manhattanda.org/sites/default/files/7.8.15%20DA%20Vance%20Written%20Testimony%20re%20Encryption.pdf.

144. Andy Greenberg, "Manhattan DA: Iphone Crypto Locked Out Cops 74 Times," *Wired*, July 8, 2015, http://www.wired.com/2015/07/manhattan-da-iphone-crypto-foiled-cops-74-times/.

145. Cyrus Vance, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy."

146. "Data Privacy and Public Safety," *International Association of Chiefs of Police*, accessed February 18, 2016, http://www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf.

147. James Comey, "Going Dark: Are technology, Privacy, and Public Safety on a Collision Course?"

148. Cyrus Vance, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy."

149. Ibid.

150. Michael Isikoff, “NSA chief: ‘Paris would not have happened’ without encrypted apps,” *Yahoo!*, February 17, 2016, https://www.yahoo.com/politics/nsa-chief-paris-would-not-have-happened-without-184040933.html.
151. Jim Yardley et al., “Inquiry Finds Mounting Proof of Syria Link to Paris Attacks,” *New York Times*, November 15, 2015, http://www.nytimes.com/2015/11/16/world/europe/inquiry-finds-mounting-proof-of-syria-link-to-paris-attacks.html.
152. Pierre Thomas, “Feds Challenged by Encrypted Devices of San Bernardino Attackers,” *ABC News*, December 9, 2015, http://abcnews.go.com/US/feds-challenged-encrypted-devices-san-bernardino-attackers/story?id=35680875.
153. John Brennan, “CIA Director John Brennan Remarks on Global Security,” *CSPAN*, video, November 16, 2015, http://www.c-span.org/video/?400755-1/cia-director-john-brennan-remarks-global-security&start=2685; Nicholas Watt, Rowena Mason, and Ian Traynor, “David Cameron pledges anti-terror law for internet after Paris attacks,” *The Guardian*, January 12, 2015, http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg.
154. Cyrus Vance et al., “When Phone Encryption Blocks Justice,” *New York Times*, August 11, 2015, http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html; Nakashima and Miller, “Why it’s hard to draw a line between Snowden and the Paris attacks,” *Washington Post*, November 19, 2015, https://www.washingtonpost.com/world/national-security/why-its-hard-to-draw-a-line-between-snowden-and-the-paris-attacks/2015/11/18/34793ad4-8e28-11e5-baf4-bdf37355da0c_story.html.
155. Matt Olsen et al, “Don’t Panic. Making Progress on the ‘Going Dark’ Debate.”
156. Kim Zetter, “Turns Out Police StingRay Spy Tools Can Indeed Record Calls,” *Wired*, October 28, 2015, http://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/.
157. “Are my messages secure?” *WhatsApp*, accessed January 5, 2016, https://www.whatsapp.com/faq/en/general/21864047.
158. Matt Olsen et al, “Don’t Panic. Making Progress on the ‘Going Dark’ Debate.”
159. Amy Hess, “Encryption and Cyber Security for Mobile Electronic Communication Devices,” *Federal Bureau of Investigations*, April 29, 2015, https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices.
160. Catherine Tsai and Solomon Banda, “Najibullah Zazi Terror Probe: A Timeline Of Events,” *Associated Press*, September 21, 2009, http://www.huffingtonpost.com/2009/09/21/najibullah-zazi-terrorpr_n_294035.html.
161. “If you see something, say something,” *U.S. Department of Homeland Security*, accessed February 11, 2016, http://www.dhs.gov/see-something-say-something/about-campaign.
162. Mike Levine, “AWOL Soldier Arrested in What Police Say Was New Fort Hood Terror Plot,” *FOX News*, July 28, 2011, http://www.foxnews.com/us/2011/07/28/exclusive-us-military-serviceman-arrested-in-second-alleged-attack-on-ft-hood/; “Oregon Resident Convicted in Plot to Bomb Christmas Tree Lighting Ceremony,” *Federal Bureau of Investigations*, news release, January 31, 2013, https://www.fbi.gov/portland/press-releases/2013/oregon-resident-convicted-in-plot-to-bomb-christmas-tree-lighting-ceremony; Neal Boudette, Andy Pasztor, and Peter Spiegel, “Bomb Attempt on U.S.-Bound Flight,” *Wall Street Journal*, December 26, 2009, http://www.wsj.com/articles/SB126178158688405369.
163. David Sanger and Nicole Perlroth, “F.B.I. Chief Says Texas Gunman Used Encryption to Text Overseas Terrorist,” *New York Times*, December 9, 2015, http://www.nytimes.com/2015/12/10/us/politics/fbi-chief-says-texas-gunman-used-encryption-to-text-overseas-terrorist.html.
164. Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, “A Worldwide Survey of Encryption Products,” *Schneier on Security*, February 2016, https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf.
165. Amir Mizroch, “In Belgium, an Encryption Powerhouse Rises,” *Wall Street Journal*, December 10, 2015, http://www.wsj.com/articles/in-belgium-an-encryption-powerhouse-rises-1449791014; 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.
166. “Encryption Technology and Terrorism,” *U.S. Senate Select Committee on Intelligence*, video, July 8, 2015, http://www.intelligence.senate.gov/hearings/counterterrorism-counterintelligence-and-challenges-going-dark.

167. "How Al-Qaeda uses Encryption Post-Snowden (Part 1)," *Recorded Future*, May 8, 2014, https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/.
168. Ellen Messmer, "Al-Qaeda group claims to have strengthened its encryption security," *Network World*, January 23, 2008, http://www.networkworld.com/article/2282593/lan-wan/al-qaeda-group-claims-to-have-strengthened-its-encryption-security.html.
169. "How Al-Qaeda uses Encryption Post-Snowden (Part 1)," *Recorded Future.*
170. Sanger and Perlroth, "F.B.I. Chief Says Texas Gunman Used Encryption to Text Overseas Terrorist."
171. "What we are talking about is the individual companies, many of which are already doing this right now for their own business purposes or other security purposes, while still maintaining strong encryption. What we are asking is that public safety and national security also be one of the factors that industry considers when determining what type of encryption to use." See, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," *U.S. Senate Committee on the Judiciary*, 101-103min; Dan Froomkin and Jenna McLaughlin, "Comey Calls on Tech Companies Offering End-to-End Encryption to Reconsider 'Their Business Model'," *The Intercept*, December 9, 2015, https://theintercept.com/2015/12/09/comey-calls-on-tech-companies-offering-end-to-end-encryption-to-reconsider-their-business-model/.
172. Daniel Conley, "Encryption Technology and Potential U.S. Policy Responses."
173. "Encryption Technology and Terrorism," *U.S. Senate Select Committee on Intelligence*, video, 25min.
174. Richard Burr, "The Debate Over Encryption: Stopping Terrorists From 'Going Dark'."
175. Ariel Rabkin, "Encryption: Conflating two technical issues in one policy debate," *Tech Policy Daily*, December 10, 2015, http://www.techpolicydaily.com/technology/encryption-conflating-two-technical-issues-in-one-policy-debate/.
176. Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity By Requiring Government Access To All Data and Communications."
177. Matt Olsen et al, "Don't Panic. Making Progress on the 'Going Dark' Debate."
178. Leonard Law, "Bring Your Own Encryption Keys to Google Cloud Platform," *Google Cloud Platform Blog*, July 28, 2015, http://googlecloudplatform.blogspot.com/2015/07/Bring-Your-Own-Encryption-Keys-to-Google-Cloud-Platform.html.
179. 40 U.S.C. § 1401, Clinger Cohen Act, *Justia*, http://law.justia.com/codes/us/1996/title40/chap25/sec1401.
180. Susan Landau, "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law & Policy*, Vol. 7, September 29, 2014, http://jnslp.com/wp-content/uploads/2015/03/NSA%E2%80%99s-Efforts-to-Secure-Private-Sector-Telecommunications-Infrastructure_2.pdf.
181. Amy Hess, "Encryption and Cyber Security for Mobile Electronic Communication Devices," *Federal Bureau of Investigations*, April 29, 2015, https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices.
182. "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," *U.S. Senate Committee on the Judiciary*, 45min.
183. Jon Brodkin, "Hillary Clinton wants "Manhattan-like project" to break encryption," *Ars Technica*, December 21, 2015, http://arstechnica.com/tech-policy/2015/12/hillary-clinton-wants-manhattan-like-project-to-break-encryption/.
184. Kif Lewing, "GOP Debate: What Republicans Got Wrong About Technology," *Fortune*, December 16, 2015, http://fortune.com/2015/12/16/republican-debate-wrong-technology/.
185. Editorial Board, "Compromise needed on smartphone encryption," *Washington Post,* October 3, 2014, https://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html.
186. Editorial Board, "Putting the digital keys to unlock data out of reach of authorities," *Washington Post,* July 18, 2015, https://www.washingtonpost.com/opinions/putting-the-digital-keys-to-unlock-data-out-of-reach-of-authorities/2015/07/18/d6aa7970-2beb-11e5-a250-42bd812efc09_story.html.
187. Lorenzo Franceshi-Bicchierai, "Congress Will Create a Commission on Encryption, Tech, and Terrorism," *Motherboard*, December 7, 2015, http://motherboard.vice.com/read/congress-will-create-a-commission-on-encryption-tech-and-terrorism.
188. Jake Laperruque and Joseph Lorenzo Hall, "FBI's New Crypto Plan: Ditch Legislation, Build Thor's Magic Hammer," *Center for Democracy and Technology*, July 9, 2015, https://cdt.org/blog/fbis-new-crypto-plan-build-thors-magic-hammer/.

189. The FBI has also cited a number of other cases involving phones that it would like Apple to unlock. See, Devlin Barrett, “Justice Department Seeks to Force Apple to Extract Data From About 12 Other iPhones,” *Wall Street Journal*, February 23, 2016, http://www.wsj.com/articles/justice-department-seeks-to-force-apple-to-extract-data-from-about-12-other-iphones-1456202213;Erin Kelly, “FBI says San Bernardino terrorist's phone still locked due to encryption,” *USA Today*, February 9, 2016, http://www.usatoday.com/story/news/2016/02/09/fbi-says-san-bernardino-terrorists-phone-still-locked-due-encryption/80074292/.

190. Ellen Nakashima, “Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks,” *Washington Post*, February 17, 2016, https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html.

191. Tim Cook, “A Message to Our Customers,” *Apple*, February 16, 2016, https://www.apple.com/customer-letter/ and Apple, “Notice of Objections To February 16, 2016 Order Compelling Apple Inc. To Assist Agents In Search,” *Cryptome*, March 1, 2016, https://cryptome.org/2016/03/usg-apple-019.pdf.

192. Timothy Lee, “Apple's battle with the FBI over iPhone security, explained,” *Vox*, February 17, 2016, http://www.vox.com/2016/2/17/11037748/fbi-apple-san-bernardino.

193. Models with 5S and newer include a “secure enclave,” which incorporates three keys: the passcode, the device-specific key, and a unique key generated by the secure enclave. In addition, this mechanism has its own timer that automatically regulates the amount of time between incorrect guesses. See, Ben Thompson, “Apple Versus the FBI, Understanding iPhone Encryption, The Risks for Apple and Encryption,” *Stratechery*, February 17, 2016, https://stratechery.com/2016/apple-versus-the-fbi-understanding-iphone-encryption-the-risks-for-apple-and-encryption/.

194. Paul Jorgensen et al., “The Patriot Act – An Impact Analysis,” *Grande Valley State University*, December 11, 2003, http://scholarworks.gvsu.edu/cgi/viewcontent.cgi?article=1128&context=cistechlib.

195. Abelson et al., “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption.”

196. Daniel Castro and Alan McQuinn, “Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness,” *Information Technology and Innovation Foundation*, June 9, 2015, https://itif.org/publications/2015/06/09/beyond-usa-freedom-act-how-us-surveillance-still-subverts-us-competitiveness.

197. Derek du Preez, “Birst partners with AWS in Ireland in direct response to NSA concerns,” *Diginomica*, August 28, 2014, http://diginomica.com/2014/08/28/birst-partners-aws-ireland-direct-response-nsa-concerns/.

198. Alonso Soto and Brian Winter, “UPDATE 3-Saab wins Brazil jet deal after NSA spying sours Boeing bid,” *Reuters*, December 18, 2013, http://www.reuters.com/article/brazil-jets-idUSL2N0JX17W20131218.

199. Leila Abbound and Paul Sandle, “Analysis: European cloud computing firms see silver lining in PRISM scandal,” *Reuters*, June 17, 2013, http://www.reuters.com/article/2013/06/17/us-cloud-europe-spyinganalysis-idUSBRE95G0FK20130617; Mitch Wagner, “Cloudwatt Builds Snoop Proof Cloud,” *Light Reading*, July 31, 2014, http://www.lightreading.com/carrier-sdn/cloudwatt-builds-snoop-proofcloud/d/d-id/710181.

200. Sara Zaske, “While US and UK governments oppose encryption, Germany promotes it. Why?” *ZDNet*, October 26, 2015, http://www.zdnet.com/article/while-us-and-uk-govts-oppose-encryption-germany-promotes-it-why/.

201. Anandita Singh Mankotia, “Government, BlackBerry dispute ends,” *Times of India*, June 10, 2013, http://timesofindia.indiatimes.com/tech/tech-news/Government-BlackBerry-dispute-ends/articleshow/20998679.cms; Barry Meier and Robert Worth, “Emirates to Cut Data Services of BlackBerry,” *New York Times*, August 1, 2010, http://www.nytimes.com/2010/08/02/business/global/02berry.html.

202. Paul Mozur, “Jitters in Tech World Over New Chinese Security Law,” *New York Times*, July 2, 2015, http://www.nytimes.com/2015/07/03/business/international/jitters-in-tech-world-over-new-chinese-security-law.html.

203. Jeff Mason, “Exclusive: Obama sharply criticizes China's plans for new technology rules,” *Reuters*, March 3, 2015, http://www.reuters.com/article/us-usa-obama-china-idUSKBN0LY2H520150303#ImrlMxxv6vpmPU4q.97.

204. Tim Culpan, "China Says Push for Companies' Encryption Keys Follows U.S. Lead," *Bloomberg Business*, March 4, 2015, http://www.bloomberg.com/news/articles/2015-03-04/china-says-push-for-companies-encryption-keys-follows-u-s-lead.
205. Paul Mozur, "China Tries to Extract Pledge of Compliance From U.S. Tech Firms," *New York Times*, September 16, 2015, http://www.nytimes.com/2015/09/17/technology/china-tries-to-extract-pledge-of-compliance-from-us-tech-firms.html; "China passes new national security law extending control over Internet," *The Guardian*, July 1, 2015, http://www.theguardian.com/world/2015/jul/01/china-national-security-law-internet-regulation-cyberspace-xi-jinping.
206. "US, Japan, EU team up to warn China of concerns over new security laws," *The Guardian*, February 29, 2016, http://www.theguardian.com/world/2016/mar/01/us-japan-eu-team-up-to-warn-china-of-concerns-over-new-security-laws.
207. Alan Travis, "Investigatory powers bill: snooper's charter to remain firmly in place," *The Guardian*, November 2, 2015, http://www.theguardian.com/world/2015/nov/02/investigatory-powers-bill-snoopers-charter-will-remain-firmly-in-place.
208. Toby Helm and Jamie Doward, "Theresa May forced to backtrack on Internet 'snooping' plans," *The Guardian*, October 31, 2015, http://www.theguardian.com/world/2015/oct/31/theresa-may-backtracks-on-internet-snooping.
209. "Investigatory Powers Bill: technology issues," *House of Commons Science and Technology Committee*, 2015, http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf.
210. Patrick O'Neill, "U.K. surveillance bill would effectively ban strong encryption," *The Daily Dot*, November 4, 2015, http://www.dailydot.com/politics/uk-investigatory-powers-bill/.
211. Basically, if one country prohibits effective encryption, then all communications that comply with that country's laws will be compromised. See, Peter Swire, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," *U.S. Senate Committee on the Judiciary*, July 8, 2015, https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf.
212. Ibid.
213. Salman Waris, "Encryption in India," *Indian Lawyer 250*, June 6, 2013, http://indianlawyer250.com/features/article/81/encryption-india/.
214. Ryan Hagemann, "The NSA and the NIST: A Toxic Relationship," *Niskanen Center*, February 9, 2016, https://niskanencenter.org/blog/the-nsa-and-nist-a-toxic-relationship/.
215. "NSA/CSS Commercial Solutions Center," *U.S. National Security Agency*, accessed January 8, 2016, https://www.nsa.gov/business/programs/ncsc.shtml.
216. Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times*, September 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0.
217. Secure Data Act of 2015, S. 135, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/135.
218. The Ensuring National Constitutional Rights of Your Private Telecommunications (ENCRYPT) Act of 2016, H.R. 4528, 114th Cong. (2016), https://cdn0.vox-cdn.com/uploads/chorus_asset/file/6025609/LIEU_027_xml__ENCRYPT_Act_of_2016_.0.pdf.
219. "Discovering IT problems, Developing Solutions, Sharing Expertise," *National Security Agency*, October 30, 2015, https://www.nsa.gov/public_info/news_information/2015/ncsam/discovering_solving_sharing_it_solutions.shtml.
220. The legal question as to whether law enforcement can compel a suspect to decrypt information has still not been settled. A potential law could spell out the specific circumstances under which law enforcement can use this tactic, narrowing the scope of these powers while offering Fifth Amendment protections.
221. Dan Terzian, "The Fifth Amendment, Encryption, and the Forgotten State Interest."
222. "About," *National Computer Forensics Institute*, accessed January 29, 2016, https://www.ncfi.usss.gov/ncfi/pages/about.jsf.
223. "Cyber Task Forces," *U.S. Federal Bureau of Investigations*, accessed January 29, 2016, https://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1.
224. After searching through legal databases, Jonathan Mayer found scant legal precedence, including five public court orders, four judicial opinions and little scholarly treatment devoted to the government's

ability to hack into systems or employ malware. See, Jonathan Mayer, "Constitutional Malware," *SSRN*, July 20, 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2633247.

225. The Federal Rules of Criminal Procedure are the rules that dictate how federal criminal prosecutions are conducted in U.S. district courts and the trial courts of the U.S. government. These rules govern how and when the government can seek access to information in the course of investigations. "Meeting Minutes," *Criminal Rules Advisory Committee*, March 16-17, 2015, http://www.uscourts.gov/file/17944/download.

226. "Details of Treaty No.185: Convention on Cybercrime," *Council of Europe*, 2001, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

227. Daniel Castro, "The False Promise of Data Nationalism," *Information Technology and Innovation Foundation*, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

ACKNOWLEDGMENTS

The authors wish to thank the following individuals for providing input to this report: Robert Atkinson, Randolph Court, and Bruce Heiman. Any errors or omissions are the authors' alone.

ABOUT THE AUTHORS

Daniel Castro is vice president of ITIF. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office where he audited IT security and management controls at various government agencies. 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.

Alan McQuinn is a research assistant at ITIF. His research areas include a variety of issues related to emerging technology and Internet policy, such as cybersecurity, privacy, virtual currencies, e-government, and commercial drones. Prior to joining ITIF, McQuinn was a telecommunications fellow for Representative Anna Eshoo (D-CA) and an intern for the Federal Communications Commission in the Office of Legislative Affairs. He got his B.S. in Political Communications and Public Relations from the University of Texas at Austin.

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 one of the world's leading science and technology think tanks, 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 ITIF.ORG.