June 2016

GOING DARK, GOING FORWARD

A PRIMER ON THE ENCRYPTION DEBATE

HOUSE HOMELAND SECURITY COMMITTEE MAJORITY STAFF REPORT

HOMELAND SECURITY
COMMITTEE

CONTENT

Executive Summary

Public engagement on encryption issues surged following the 2015 terrorist attacks in Paris and San Bernardino, particularly when it became clear that the attackers used encrypted communications to evade detection—a phenomenon known as "going dark." While encryption provides important benefits to society and the individual, it also makes it more difficult for law enforcement and intelligence professionals to keep us safe.

Some have framed the debate surrounding encryption as a battle between privacy and security. Our extensive discussions with stakeholders, however, have led us to conclude that the issue is really about security versus security: encryption protects critical infrastructure, trade secrets, financial transactions, and personal communications and information. Yet encryption also limits law enforcement's ability to track criminals, collect evidence, prevent attacks, and ensure public safety. Initially, lawmakers and some among law enforcement personnel believed the solution was simple: statutorily authorize law enforcement access to obtain encrypted data with a court order. Unfortunately, this proposal was riddled with unintended consequences, particularly if redesigning encryption tools to incorporate vulnerabilities—creating what some refer to as "backdoors"—actually weakened data security. Indeed those vulnerabilities would naturally be exploited by the bad guys—and not just benefit the good guys.

The global technology industry is undergoing rapid change. Consumers now demand that companies incorporate encryption into their products and services as a matter of routine practice. We are just beginning to understand the implications of this transformation. If the U.S. placed burdensome restrictions on encryption, American technology companies could lose their competitive edge in the global marketplace. Moreover, studies suggest that two-thirds of the entities selling or providing encrypted products are outside of the United States. Thus, bad actors could still obtain the technology from foreign vendors irrespective of U.S. legislative action.

Over the course of the past 12 months, Members and staff of the House Committee on Homeland Security have held more than 100 meetings and briefings, both classified and unclassified, with key stakeholders impacted by the use of encryption. As a result of our robust investigation, the Committee staff has come to understand that there is no silver bullet regarding encryption and "going dark." While we benefited tremendously from our engagement with stakeholders, we did not discover any simple solutions. No matter what path emerged, there were always troublesome trade-offs. Thus, in our estimation, the best way for Congress and the nation to proceed at this juncture is to formally convene a commission of experts to thoughtfully examine not just the matter of encryption and law enforcement, but law enforcement's future in a world of rapidly evolving digital technology.

We believe that experts in the fields of commercial technology, computer science and cryptology, privacy and civil liberties, law enforcement, intelligence, and global economics are best equipped to deconstruct this extraordinarily complex problem, and propose novel solutions that will stand the test of time. House Homeland Security Chairman Michael McCaul (R-TX) and Senator Mark Warner (D-VA) have proposed the formation of a ***National Commission on Security and Technology Challenges*** (hereinafter, "Digital Security Commission") to bring these experts together to engage one another directly and, over the course of a year, develop policy and legislative recommendations to present to Congress. The report the Commission will produce will also serve as an invaluable reference document, providing a better understanding of this issue for Congress and the American public, and helping to forge a national consensus on solutions that preserve American innovation, strengthen our competitiveness, and preserve the rule of law.

The Committee has produced this primer to briefly describe important themes and considerations surrounding the widespread use of encryption technologies—including the practical and economic value encryption brings to certain industries and the wider market; the impact ubiquitous encryption is having on law enforcement; the ways in which various governments around the world are responding to this challenge; and a discussion of some existing legislative proposals. Finally, this document explains why future progress in addressing these challenges will likely depend on a more formal national discussion involving the necessary stakeholders in the form of a national commission on digital security.

Committee members & staff held over **100 meetings on this issue** with technology industry leaders; the Intelligence Community, State, local & Federal law enforcement associations & agencies; District Attorneys & Prosecutors; privacy advocates; cryptologists, technologists & academics; & foreign data protection officials.

This effort has included classified briefings, site visits, roundtables, & research.

Over the course of the past year, **the Committee has received the input of concerned voices across Congress & across the country.**

Introduction

American innovation and ingenuity has spurred the development of technologies that make it easier to travel, communicate, research, create, produce and distribute quality goods, and generally improve quality of life—not only for Americans, but for people around the world. So too, since our founding, the U.S. has been dedicated to preserving and expanding the rule of law, including the pursuit of justice at home and the promotion of American values abroad. These two ideas have remained hallmarks of the American identity for nearly two hundred and fifty years. Even today, they jointly continue to inform our progress toward a "more perfect union."

Yet, through the course of our history, the concepts of innovation and regulation have sometimes seemed at odds with one another. Congress and the American people have always sought to strike the right balance between the rule of law and individual liberty. Several examples illustrate this point, including debates surrounding the development of a robust anti-money laundering regime in online and in-person banking in the 1980s and 1990s; the Communications Assistance for Law Enforcement Act in the early 1990s; the appropriate use of "roving wiretaps" in response to the widespread adoption of mobile communications in the early 2000s; and current discussions on the proper role of commercial drone technology in public and private arenas.

In recent years, we have been presented with one more example of this challenge: the widespread use of encryption by the general public and the exploitation of this technology by criminals and terrorists. This debate has been accelerated by the allegations made by former federal contractor Edward Snowden regarding government surveillance and privacy and the rise of the tech-savvy Islamic State of Iraq and Syria (ISIS) and its attacks against the West. In describing the issue, Secretary of Homeland Security Jeh Johnson noted, "The current course we are on, toward deeper and deeper encryption in response to the demands of the marketplace, is one that presents real challenges for those in law enforcement and national security … We in government know that a solution to this dilemma must take full account of the privacy rights and expectations of the American public, the state of technology and the cybersecurity of American businesses."[1] Clearly, the problem at hand is complex.

According to **FBI Director James Comey**, "Going Dark" refers to the phenomenon in which law enforcement personnel have the "legal authority to intercept and access communications and information pursuant to court order," but "lack the technical ability to do so."

What's more, many stakeholders involved in the discussions surrounding this issue feel their motives, patriotism, and even their intelligence are called into question by those who oppose their point of view. As a result, relationships have been damaged and progress has been stymied.

In an effort to find solutions, the House Homeland Security Committee engaged all relevant parties to identify steps that could be taken toward a solution. The Committee held more than 100 meetings with various stakeholders—including experts from the technology industry, federal, State, and local law enforcement, privacy and civil liberties, computer science and cryptology, economics, law and academia, and the Intelligence Community. This process, which took place over the course of more than a year, revealed the significant complexities surrounding not only the use of encryption by criminals and terrorists, but also the overall challenges associated with how U.S. law enforcement and intelligence agencies adapt to rapid advances in technology.

As a result of its investigation, the Committee developed ***seven general findings***:

1. Encryption plays a vital role in modern society, and increasingly widespread use of encryption in digital communications and data management has become a "fact of life."

2. Law enforcement entities face real and persistent challenges when they encounter encrypted communications during the course of investigations and prosecutions. In some situations, encryption restricts law enforcement's ability to successfully prosecute cases or to identify and mitigate threats to public safety and national security.

3. Today, more than ever before, technology, public safety, and counterterrorism are inextricably linked. Technology, such as encryption, protects our data and our infrastructure, and helps to ensure the privacy of our citizens; yet it is also exploited by bad actors, including drug traffickers, child predators, and terrorists, to facilitate criminal activities, and threaten our national security. Thus, what we are really dealing with is not so much a question of "privacy versus security," but a question of "security versus security."

4. Governments worldwide are struggling to address the challenge of "security versus security," and are exploring multiple policy and legislative responses. This is resulting in a patchwork of inconsistent laws and proposals governing the same issue to the detriment of law-abiding citizens and the benefit of criminals and terrorists.

5. Any legislative "solutions" yet proposed come with significant trade-offs, and provide little guarantee of successfully addressing the issue. Lawmakers need to develop a far deeper understanding of this complex issue before they attempt a legislative fix.

6. The impacted parties themselves need to directly engage one another in an honest and in-depth conversation in order to develop the factual foundation needed to support sustainable solutions.

7. The debate surrounding the abuse of widely available encryption technology is part of a larger question of ensuring that law enforcement and national security efforts keep pace with technological advancement without undermining American competitiveness and American values.

I. Encryption, Security, and the Modern Economy

Smartphones

The speed with which society has absorbed mobile communication devices and sophisticated communication platforms into daily life is staggering. Only a few years ago, cell phone capabilities were normally limited to phone calls and text messages. But according to a survey released in April 2015, nearly two thirds of Americans now own a smartphone that provides Internet access and stores vast amounts of personal data.[2] A separate report suggests there are approximately 2.6 billion smartphone subscriptions worldwide.[3]

2.6 BILLION
smartphone subscriptions worldwide

Because a single device can now contain a phone, camera, and global positioning system (GPS), as well as access to email, social media, and web browsing, and can store sensitive information like health records and financial data, users have come to expect their devices to be secure. Therefore, many smartphone users rely on password protection, encryption, and other security features to safeguard the content of their devices. In many ways, the smartphone has reshaped our thinking about privacy and security.

At its most basic, **encryption** is a process of limiting access to data by "using a code or mathematical algorithm so as to [make the data] unintelligible to unauthorized readers."

The American Heritage Science Dictionary

The Internet

A 2012 report published by the Boston Consulting Group estimated that by 2016, half the world's population will be using the Internet, and the value of the Internet within the G-20 economies would reach $4.2 trillion.[4] According to the Internet Association, in 2014, the Internet sector contributed $966.2 billion to the U.S. economy, or 6 percent of real GDP.[5] Today, more than half the world's population—and 84 percent of American adults—use the Internet.[6]

Moreover, the physical world is becoming increasingly connected to the Internet. From critical infrastructure systems like water treatment plants and electrical grids, to financial institutions, to new models of automobiles and everyday household appliances, the

"internet of things" (IoT) is on the rise. This has created new concerns about the security of networks. As more and more consumer facing "things" become interconnected, the public will likely demand that encryption be made available for everyone and everything.

Impact on the Modern Economy

Nearly every aspect of the modern economy benefits from advancements in digital communications—and the security of those communications is critical. A 2016 study from the Ponemon Institute reports that 85 percent of more than 5,000 information technology (IT) professionals surveyed globally said that their organizations have an encryption strategy, and 37 percent said it was applied consistently across the enterprise.[7] This is a substantial increase from a survey Ponemon conducted in 2005 which found that an astounding 38 percent of U.S. organizations had no encryption strategy in place at all.[8]

While it is not possible to quantify exactly how much economic growth has been supported by the use of encryption, it is generally accepted that the ability of major firms to protect their customers' data will continue to be an important factor. Thus far, the evidence suggests that Americans have clearly embraced encryption as the best means to safeguard their information and transactions online.

Impact on Financial Services

Banks and other financial institutions invest heavily in encryption technologies to protect their networks and safeguard their information. In fact, due in part to regulatory demands and best practices, the "financial sector accounts for approximately 44 [percent] of [the] global encryption software market," according to a recent report.[9] American consumers expect their financial data to remain both accessible and secure.

***44%** of encryption software market is for financial services*

***30 MILLION** households use online banking on mobile devices*

Indeed, 51 percent of U.S. adults, or 61 percent of Internet users, bank online. And, as of 2013, approximately 30 million households report using online banking through mobile devices.[10] The banking and financial services industry has long been recognized as a leader in security. As a 2011 survey from the analytics firm comScore points out, "customers still reported feeling more secure on their [financial institution's] website than on the Internet as a whole."[11]

This confidence in online banking has sparked innovation and improvements over time. A Federal Reserve Payments Study from 2013 found that although paper checks continue "to persist as a significant portion of noncash payments … interbank processing and clearing of these checks are virtually all electronic."[12] Without strong encryption protecting these

transfers, the number of fraudulent transactions would undoubtedly be significantly higher. Data breaches for financial institutions are among the primary motivations for the industry's heavy investment in encryption.

Impact on E-commerce and Retail

Mirroring trends in online banking and financial services, online commerce would be far less trusted and far less robust without encryption to keep customer data secure for payment processing. In 2015, the Department of Commerce estimated e-commerce sales at $341.7 billion, accounting for 7.3 percent of total retail sales—a 14.6 percent increase from 2014.[13] E-commerce has become a critical component of the U.S. economy. According to the most current data available, in 2013 U.S. manufacturers reported that e-commerce shipments were valued at approximately $3.3 trillion.[14][15]

$341.7 BILLION
e-commerce sales in 2015

Impact on Healthcare

Since 2009, the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule has encouraged healthcare providers to secure their data through encryption by requiring those that suffer a data breach to notify their clients within 60 days.[16] Despite this move, the American health system has fallen victim to a number of high-profile data breaches. According to the Department of Health and Human Services Office of Civil Rights, which publicly reports breaches affecting more than 500 individuals, 253 breaches compromised 112 million total records in 2015. Moreover, the International Data Corporation's Health Insights group predicts "1 in 3 health care recipients will be the victim of a health care data breach in 2016."[17]

1 IN 3
health care recipients will be the victim of a health care data breach in 2016

II. Encryption, Public Safety, and Law Enforcement

The Digital Crime Scene

Although digital technology has brought value to the marketplace, the proliferation of applications and devices that utilize end-to-end encryption has presented law enforcement and intelligence officials with new challenges: criminals, terrorists, and other bad actors are taking advantage of encryption to hide their activities, operate in the dark, and conceal evidence. Because so much information—communications, records, photographs, etc.—is now stored on personal digital devices like smartphones and personal computers, law enforcement professionals are increasingly investigating "digital crime scenes." Accordingly, law enforcement and intelligence officials have reported to Committee staff that their inability to obtain access to the digital communications of criminals is increasingly hindering their activities. Indeed, the Office of the District Attorney for New York County reported that investigators struggled with more than 175 cases between September 2014 and March 2016 because they lacked access to digital information.

At the same time, Federal Bureau of Investigation (FBI) **Director James Comey** testified before the House Homeland Security Committee in the fall of 2015 that:

> *Unfortunately, changing forms of Internet communication and the use of encryption are posing real challenges to the FBI's ability to fulfill its public safety and national security missions. This real and growing gap, to which the FBI refers as "Going Dark," is an area of continuing focus for the FBI; we believe it must be addressed given the resulting risks are grave both in traditional criminal matters as well as in national security matters.*[18]

Compelling Assistance

The government has relied on the *1789 All Writs Act ("AWA")* to help law enforcement gain access to certain encrypted communications. Absent alternative remedies, the AWA authorizes U.S. federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." In other words, under certain circumstances, the court can compel a private entity to provide assistance to the government.

Unable to technically access data on a device despite a lawful warrant, law enforcement requests often rely on the AWA to compel technology companies to assist in data recovery. This has raised the question of whether the AWA may be used to compel a company to provide a "key" to an encrypted device or write code to bypass security features. Over the past several years, the government

has increasingly utilized the law to compel technology companies, like Apple and Google, to help law enforcement execute search warrants for investigations.

A recent American Civil Liberties Union (ACLU) report documented 63 confirmed cases since 2008 across the country in which the government has applied for AWA assistance from Google or Apple to assist in data recovery.[19] New York and California reported the highest number of filings, with 12 and 16 cases respectively.[20] The filings identified by the report largely consist of requests for assistance in bypassing locked screens, resetting passwords, creating code, and extracting data.[21] According to the ACLU, investigations into drug related crimes appear to be the leading cause of AWA motions.[22] Other motions filed involved investigations into credit fraud, identity fraud, bribery, child pornography, and human trafficking charges.[23]

Still, it would be a mistake to suggest that the officials charged with investigating and prosecuting criminals and terrorists and protecting the American public do not understand the value of encryption. The FBI, the Department of Homeland Security (DHS), and the wider Intelligence Community use strong encryption to secure their own information. Indeed, senior U.S. officials are on record encouraging the private sector and the public to do the same.[24] At a Senate Hearing in July 2015, FBI Director Comey and Deputy Assistant Attorney General Sally Quillian Yates testified that the development and adoption of strong encryption is key to securing commerce and trade, safeguarding private information, promoting free expression and association, and strengthening cyber security.[25] They stated that, "DOJ and the FBI support and encourage the use of secure networks to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data so as to promote our overall safety."[26]

Court Authorization to Conduct Electronic Surveillance

It is important to remember that only a handful of offenses are serious enough to justify electronic interception orders. To obtain such an order, investigators must demonstrate that normal investigative procedures are impossible, or too dangerous to use. Additionally:

- Intercept orders have a limited scope;
- Targets of the surveillance must be identified with specificity; and
- Requests are subject to review by a U.S. Attorney, and by the Attorney General or Deputy Assistant Attorney General prior to being submitted to the Courts.

These authorities are granted under Title III of the Wiretap Act (for criminal cases) and the Foreign Intelligence Surveillance Act (FISA) for cases involving foreign powers and the agents of foreign powers.

Encryption and Terrorism

Unfortunately, terrorists also use encryption technology to hide their communications from law enforcement and intelligence professionals. FBI Director Comey recently testified to the Senate Judiciary Committee that when ISIS operatives encounter a potential recruit, "we see them giving directions" to move to a mobile messaging app that is encrypted. "And they disappear."[27] In later testimony, Comey further commented, "There is no doubt that the use of *encryption is part of terrorist tradecraft now* because they understand the problems we have getting court orders to be effective when they're using these mobile messaging apps, especially that are end-to-end encrypted" [emphasis added].[28] Indeed, the perpetrators of terrorist attacks in Garland, Texas, Paris, France, and San Bernardino, California, in 2015 all exploited encrypted communications.

> "There is no doubt that the use of encryption is part of terrorist tradecraft now because they understand the problems we have getting court orders to be effective when they're using these mobile messaging apps, especially that are end-to-end encrypted."
>
> FBI Director James Comey
> December 9, 2015

Yet this phenomenon is not new. Law enforcement and intelligence agents have been grappling with terrorists' use of encryption for more than a decade. Though it is difficult to verify, according to one report, attackers in Bali, Madrid, and London masked their communications with encryption.[29] The difference is that now, in 2016, encryption is ubiquitous. "The proficiency of criminals with encryption technology has advanced a lot [over the years] and smartphones now have the same parts as the PCs of 15 years ago," commented Ran Canetti, a cryptography expert and professor at Boston University. "Strong encryption is widespread. Everybody today who wants to get their hands on strong encryption mechanics, they can do it." Moreover, Canetti continued, "There's no way to prevent people from using encryption. The 10 percent who would want the encryption secrecy will find a way to get it." Thus, he concludes, "[Law enforcement] developing better encryption-cracking tools is a very good thing. But they should concentrate on encryption made by bad guys. Making the everyday encryption of the general public weak isn't going to get you what you want, [not] when it comes to coordinated terrorist attacks. There's no silver bullet answer."[30]

III. Encryption Around the Globe: A Patchwork of Legislative Responses

The 2015 terrorist attacks in Paris and San Bernardino prompted legislators across the globe to consider the challenges created by widespread use of end-to-end encryption. Different countries adopted different approaches to address the issue, creating a patchwork of laws and regulations.

United Kingdom

The United Kingdom (U.K.) in November 2015 introduced the Investigatory Powers bill in Parliament. While the bill seeks primarily to grant authorities to the government for bulk collection and lawful hacking, there are also elements addressing digital communications technology. According to news reports, "the bill gives the government the power to order 'the removal of electronic protection applied by a relevant operator to any communications or data.'"[31] The exact meaning of this and other terminology has been under scrutiny from lawmakers inside the British government. In February 2016, the Science and Technology Committee in the House of Commons released a report criticizing the bill for its lack of clarity on terms and definitions, as well as the potential impact on privacy, technology, and encryption.[32] The Chair of the Committee, Nicola Blackwood, reiterated her support for encryption and opposed any "backdoor" or other exceptional accesses.[33]

On June 7, 2016, the House of Commons passed an updated version of the Investigatory Powers bill in a 444-69 vote.[34] While it upholds the bulk surveillance and computer hacking authorities, the final version includes additional privacy protections and clarification that companies are not required to provide the government with access to encrypted communications unless it is technically feasible and not unduly expensive.[35] These additions helped the bill gain broader support than it had upon introduction, but the bill still faces some opposition from privacy groups.[36] The House of Lords will now consider the bill with a decision expected later in 2016.[37]

Additionally, press reporting in February 2016 suggested that U.S. and British officials began negotiating a bilateral agreement to update the mutual legal assistance treaty (MLAT) process for exchanging data.[38] The current MLAT process requires a foreign government to make a formal diplomatic request for data and the Justice Department to seek a court order for the data on behalf of that country. This process can take months, which many countries complain is too long, particularly in sensitive national security investigations. The new proposal "would enable the British government to serve wiretap orders directly on U.S. communications firms for live intercepts" and seek stored data on U.K. citizens.[39] The agreement would allow the U.S. government to have the same authority for data from British providers involving U.S. citizens.[40] The proposal is intended to help the U.S. obtain appropriate information from relevant British companies, as well as reduce the administrative burden on U.S companies seeking to comply with British requests.[41] Congress must approve any final agreement.

France

French legislators in January 2016 considered an amendment to the Digital Republic bill that required technology companies to provide government access to certain products.[42] The amendment was introduced in the wake of the attacks in Paris to provide law enforcement with additional tools to prevent future attacks.[43] Legislators rejected the amendment out of fear that it would ultimately weaken data security.[44]

A month later, however, the lower chamber of Parliament voted in favor of an amendment to punish tech companies that refused to decrypt messages for law enforcement.[45] The legislation included language that punished offenders with a €350,000 fine and up to five years in prison.[46] Legislators are currently pushing the bill through the legislative process.

The Netherlands

In the wake of the Paris attacks, Amsterdam began reviewing the government's law enforcement authorities and concluded it would not force technology companies to share encrypted communications.[47] The Dutch government reasoned—similar to the amendment to the French Digital Republic bill—that such a move would weaken data security and create vulnerabilities for "criminals, terrorists and foreign intelligence services" to exploit.[48]

Germany

German government officials recently expressed support for strong encryption and vowed to become "one of the most secure digital locations" in the world.[49] Officials also pledged "more and better encryption" and commented that the country aims "to be the world's leading country in this area. To achieve this goal, the encryption of private communication must be adopted as standard across the board."[50]

European Union

European Commission Vice President Andrus Ansip in May 2015 commented that there were no plans to enable access to encrypted communications in Europe.[51] Citing the importance of maintaining public trust, Ansip cautioned that if there were backdoors then someone would eventually abuse them.[52] Ansip in March 2016 reiterated his opposition to "backdoors to encrypted systems" because "sooner or later somebody will misuse [them]."[53] He also urged the U.K. and France to prevent backdoor access to encrypted technology.

China

China in December 2015 passed an antiterrorism law requiring telecommunication and Internet service providers to "provide technical interfaces, decryption and other technical support and assistance to public security and state security agencies when they are following the law to avert and investigate terrorist activities."[54] It is unclear whether the law will have any impact on U.S. companies because Beijing has yet to implement the legislation. The final law does not go as far as the initial draft, however, which would have required companies to pass proprietary information directly to the government.[55]

India

The Indian government in September 2015 withdrew a proposal that would have forced citizens to store plain-text versions of their data for 90 days and make it available to security agencies after widespread blowback from the technology sector and privacy and human rights groups.[56]

Iran

In May 2016, Iran's Supreme Council of Cyberspace set a one year deadline for foreign messaging companies to transfer all data and activity associated with Iranian users to servers in Iran.[57] This deadline has raised privacy and security concerns over storing such data within the country, where the use of messaging services is becoming widespread – including an estimated 20 million Iranians using the popular messaging app Telegram.[58]

Brazil

The Brazilian government in December 2015 sought to compel Facebook subsidiary WhatsApp to share encrypted communications with authorities in a drug trafficking investigation. When WhatsApp failed to produce the communications, a Brazilian judge ordered the company to shut down.[59] The order was overturned only hours later after public backlash.[60] With nearly 100 million WhatsApp users in Brazil,[61] "Brazilians sought temporary refuge in other communications that weren't blocked by the court order, such as Viber or Facebook Messenger. Telegram Messenger reported that some 1 million Brazilians signed up for its service within a matter of hours."[62]

Brazilian authorities later arrested a senior Facebook executive in March 2016 when WhatsApp failed to produce the same encrypted communications. [63] The executive was released after 24 hours, when a judge reversed the arrest order.[64]

United Nations

United Nations High Commissioner for Human Rights Zeid Ra'ad Al Hussein in March 2016 commented that encryption was essential to the interests of freedom.[65] He stated, "Encryption and anonymity are needed as enablers of both freedom of expression and opinion, and the right to privacy. Without encryption tools, lives may be endangered."[66] While acknowledging that law enforcement "deserves everyone's full support" in carrying out investigations, he expressed concern over "unlocking a Pandora's Box that could have extremely damaging implications for the human rights of many millions of people, including their physical and financial security."[67]

United States

As discussed above, the U.S. government has relied on the AWA to compel the assistance of private entities like Apple and Google to help the government enforce other lawful orders or decisions. Recently, Apple challenged the government's power under the AWA in two high-profile cases in New York and California, resulting in dueling orders that could set the stage for conflicting precedent in the future. The federal government ultimately withdrew its request when it discovered another way to access the devices in question.

Although to date no legislation has been enacted to address the issue, and the White House has declined to take a position, many of the stakeholders the Committee met with have strong opinions on the appropriate path forward. One view is that encryption is an essential element of an individual's right to privacy and must be protected at all costs. As the ACLU noted, "To preserve the promise of expression online, our laws must adequately protect the rights to communicate securely and to remain anonymous."

Yet others have suggested it is necessary to sacrifice *some* level of privacy to ensure that Americans are kept safe from harm. Moreover, courts generally agree that there is no absolute right to privacy in America: we operate within a system of checks and balances where the government has the right—provided it is pursued by lawful means—to obtain certain information to protect U.S. national security. Thus, companies, like any other component of our society, must abide by the same set of rules irrespective of the perceived burden.

"These issues are too important to resort to inaction, and too complex to resolve without consensus."

Edward F. Davis
Former Commissioner of the Boston Police Department
December 9, 2015

Congressional Legislative Proposals

Several bills offered in Congress reflect these strong opinions. For example, the "ENCRYPT Act of 2016", offered by Rep. Ted Lieu (D-CA) in February 2016, provides that no State or subdivision thereof may prohibit the use of encryption or compel any entity to "design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency or instrumentality of a State, a political subdivision of a State, or the United States."[68]

At the other end of the spectrum, the "Compliance with Court Orders Act of 2016," a discussion draft offered by Intelligence Committee Senators Richard Burr (R-NC) and Diane Feinstein (D-CA) in April 2016, requires that "a covered entity that receives a court order from a government for information or data shall provide such information or data to such government in an intelligible format; or provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order."[69]

A third way, offered by House Homeland Security Chairman Michael McCaul (R-TX) and Senator Mark Warner (D-VA), proposes to bring together experts from each of the key areas—cryptology, global commerce and economics, federal, State and local law enforcement, the technology sector, the Intelligence Community, and the privacy and civil liberties community—to form a Digital Security Commission. The Commission would be charged with analyzing digital security challenges, including encryption and developing recommendations for Congress to chart a co urse forward.

The McCaul/Warner Commission includes representatives from:

- Cryptology
- Global commerce and economics
- Federal law enforcement
- State and local law enforcement
- Consumer-facing technology sector
- Enterprise technology sector
- Intelligence Community
- Privacy and civil liberties community

This approach recognizes that equities on all sides of the encryption debate should be taken into consideration.

IV. No Simple Solution: Trade Offs And Trends

Two key themes have emerged from our discussions with stakeholders over the past year: 1) if we are to get ahead of this issue as a society, we must first develop a common lexicon and a common understanding of what the problem actually is; and 2) legislative proposals seem to determine clear "winners" and "losers" in the debate, thereby risking significant blowback for all the parties involved. As Director of the National Security Agency Admiral Michael Rogers recently commented:

> *Encryption is foundational to the future – given that foundation, what is the best way to deal with it? It's crazy to think we can make it go away. Technology is creating capabilities that have only been a dream for us as a society in the past, we need to figure out how to deal with that reality… Concerns about privacy have never been higher, given this combination, how do we make all of this work? We need balance realizing it isn't about one or the other. This is not just a military or national security problem, it is much broader than that.*[70]

Stakeholders have also raised legitimate questions about the impact of U.S.-centric legislation on U.S. companies' ability to compete in a global market. For example, as discussed above, a study released earlier this year conducted by Harvard University suggests that two-thirds of entities selling or providing encrypted products are outside of the United States.[71] Thus, U.S. legislation might have little impact on bad actors that can obtain encryption tools outside of the United States, while irreparably harming U.S. commercial interests by driving customers to foreign competitors. Indeed, according to the authors of the Harvard University's Berkman Center for Internet and Society paper *Don't Panic: Making Progress in the "Going Dark" Debate*, "critics fear that architectures geared to guarantee such access would compromise the security and privacy of users around the world, while also hurting the economic viability of U.S. companies."[72]

Other stakeholders have suggested that it is the transition to *default* encryption on widely available products and smartphone applications which encrypt or automatically erase communications that pose the real problem.[73] They argue, if criminals or terrorists had to proactively opt into encryption, or go out of their way to obtain encryption software, the problem might be more manageable. As Office of the Director of National Intelligence General Counsel Robert Litt recently noted, "there are a lot of sloppy and stupid terrorists out there … people don't always choose the most secure" technologies.[74]

These perspectives further illustrate the diversity of views on technology issues specifically, particularly when it comes to reaching a consensus on appropriate policy and legislative recommendations. No matter the issue, there will be trade-offs and compromises that likely need to be reached.

V. Building Consensus in the Face of Complex Challenges: A Need for National Dialogue

In the words of former Commissioner of the Boston Police Department, Edward F. Davis, "These issues are too important to resort to inaction, and too complex to resolve without consensus." Yet, to date, consensus has remained elusive. Many had hoped that a dialogue among the key stakeholder interests surrounding encryption and national security—especially in the wake of the Paris, Brussels, and San Bernardino attacks—would develop organically. But no such dialogue has begun. Still, many commentators from the tech industry, the national security and intelligence communities, academia, law enforcement, and lawmaking agree that this kind of dialogue is essential to getting beyond the rancor and solving the problem. As Ryan Hagemann, a technology and civil liberties analyst at the libertarian advocacy organization, the Niskanen Center, and Andrew Chang, co-founder and managing partner of Eastern Foundry, an incubator and accelerator for tech startups working with government wrote recently, "[a Congressionally-mandated dialogue] is the best path forward to resolving the encryption debate. By assembling a report and recommendations from the leading minds in the fields of economics, law, technology, computer science, and law enforcement, we can begin to form a general concurrence of opinions, informed by a common understanding of the underlying facts."[75]

In further support of this approach, **CIA Director John Brennan** said in his testimony before the Senate Intelligence Committee in June 2016, "I don't know what the best way is [to solve the encryption question], but I know that it has to be an effort undertaken by the government and the private sector in a very thoughtful manner that looks at the various dimensions of the problem and is going to come forward with a number of options—recommendation…A congressional commission on this issue is something that really could do a great service. There needs to be an understanding between the private sector and the government about what our respective roles and responsibilities are going to be and be able to find some kind of solution that's able to optimize what it is we're all trying to achieve."

The Committee has arrived at the same conclusion. While Congress—as opposed to the courts—is the proper forum to consider novel matters of law and policy, we recognize that this is a truly complex issue. A comprehensive report—one which will include new ideas for addressing digital security challenges—will be incredibly valuable for Members of Congress as they endeavor to make the most informed decisions possible. We further recognize that the debate surrounding encryption is itself part of a larger conversation on technological transformation and its impact on American competition, security and values. We believe the best way to make informed, sustainable decisions is to bring together experts who best understand the complexities of this issue, and can advise Congress on the best path forward. Apple CEO Tim Cook recently weighed in on a Commission proposal, noting "Our country has always been strongest when we come together. We feel the best way forward would be [to]…as some in Congress have proposed, form a commission or other

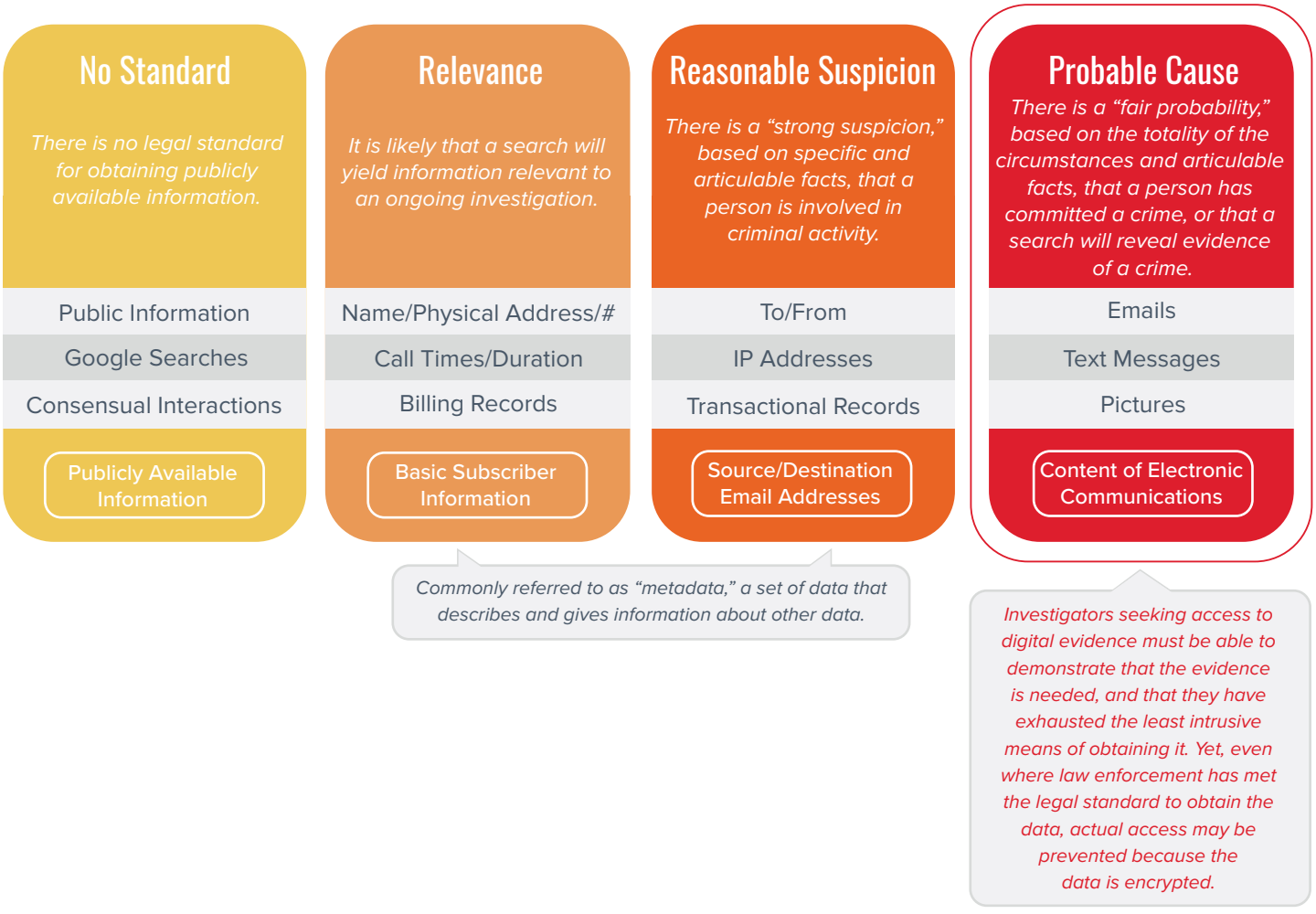
panel of experts on intelligence, technology and civil liberties to discuss the implications for law enforcement, national security, privacy and personal freedoms. Apple would gladly participate in such an effort."[76]

Former House Speaker Newt Gingrich (R-GA) and former House Intelligence Committee Member Jane Harman (D-CA) summed things up, writing in a joint Op-Ed on the issue in April 2016, "We each have private hopes, of course, that an expert, unbiased commission will recommend what we already believe. But we're willing to learn that we have things completely backward; Apple, the Obama administration and members of Congress should be just as open. The question of encryption is too central to this country's future to answer without a real dialogue."[77]

Appendix – *Legal Standards for Obtaining Digital Evidence*

When considering whether law enforcement agents should be able to access encrypted data containing evidence of a crime, it is important to remember that there are legal standards and procedural requirements in place all along the way to safeguard the privacy of Americans.

Investigators must meet a series of escalating legal standards in order to obtain various types of data. Most investigations begin by casting a wide net. As new facts emerge and evidence is gathered, the case narrows. As the data sought becomes increasingly private and potentially revealing, the standards to obtain that data become increasingly difficult to meet. Below is a diagram that helps to explain the process by associating various types of data that investigators may seek with the corresponding legal standards that must be reached.



Endnotes

1 Jeff Stone, "DHS Chief Jeh Johnson Calls Encryption A Threat To Public Safety," International Business Times, April 22, 2015. http://www.ibtimes.com/dhs-chief-jeh-johnson-calls-encryption-threat-public-safety-1892057

2 Aaron Smith, "U.S. Smartphone Use in 2015," Pew Research Center, April 2015. http://www.pewinternet.org/2015/04/01/chapter-one-a-portrait-of-smartphone-ownership/

3 Ingrid Lunden, "6.1B Smartphone Users Globally By 2020, Overtaking Basic Fixed Phone Subscriptions," Tech Crunch, June 2, 2015. http://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/#.mjrlvwq:RPIH

4 David Dean et al, "The Internet Economy in the G-20," Boston Consulting Group, 2012. https://www.bcg.com/documents/file100409.pdf

5 Stephen Siwek,"Measuring the U.S. Internet Sector," the Internet Association, December 10, 2015. https://internetassociation.org/121015econreport/

6 Andrew Perrin and Maeve Duggan, "Americans' Internet Access: 2000-2015," Pew Research Center, June 26, 2015. http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/

7 Ponemon Institute, "2016 Global Encryption Trends Study," Thales Security, February 2016. http://images.go.thales-esecurity.com/Web/ThalesEsecurity/%7B5f704501-1e4f-41a8-91ee-490c2bb492ae%7D_Global_Encryption_Trends_Study_eng_ar.pdf

8 Id.

9 "Global Encryption Software Market is Expected to Reach $2.16 Billion by 2020 - Allied Market Research," PR Newswire, January 28, 2015. http://www.prnewswire.com/news-releases/global-encryption-software-market-is-expected-to-reach-216-billion-by-2020---allied-market-research-290039391.html

10 Susanna Fox, "51% of U.S. Ad ults Bank Online," Pew Research Center, Aug. 7, 2013. http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/

11 Nathan Frederiksen and Sarah Lenart, "2011 State of Online and Mobile Banking," comScore Financial Services, February 2012. https://www.comscore.com/Insights/Presentations-and-Whitepapers/2012/2011-State-of-Online-and-Mobile-Banking

12 Gerdes, Geoffrey et al, "The 2013 Federal Reserve Payments Study," Federal Reserve System, July 2013. https://www.frbservices.org/files/communications/pdf/general/2013_fed_res_paymt_study_detailed_rpt.pdf

13 Rebecca DeNale and Deanna Weidenhamer, "U.S. Census Bureau News," U.S. Department of Commerce, February. 17, 2016. https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

14 U.S. Census Bureau, "E-Stats 2013: Measuring the Electronic Economy," U.S. Census Bureau, May 28, 2015. https://www.census.gov/econ/estats/e13-estats.pdf

15 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.pdf

16 Ricardo Alonso-Zaldivar, "Lack of encryption standards raises health data privacy

questions," Associated Press, February 8, 2015. http://www.pbs.org/newshour/rundown/lack-health-care-cyber-security-standards-raises-questions/

17 Dan Munro, "Data Breaches In Healthcare Totaled Over 112 Million Records In 2015," Forbes, December 31, 2015. http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#146c243f7fd5

18 Hon. James B. Comey, "Statement Before the House Committee on Homeland Security Washington, D.C." October 21, 2015. https://www.fbi.gov/news/testimony/worldwide-threats-and-homeland-security-challenges

19 Eliza Sweren-Becker, "This Map Shows How the Apple-FBI Fight Was About Much More Than One Phone," American Civil Liberties Union, March 2016. https://www.aclu.org/blog/speak-freely/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone

20 Id.

21 Id.

22 Id.

23 Id.

24 Federal Bureau of Investigation (FBI), "Going Dark Issue." https://www.fbi.gov/about-us/otd/going-dark-issue

25 Hon. James Comey, "Joint Statement with Deputy Attorney General Sally Quillian Yates before the Senate Judiciary Committee," July 8, 2015. https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy

26 Id.

27 Cory Bennett, "Administration spars with lawmakers over access to encrypted data," The Hill, July 8, 2015. http://thehill.com/policy/cybersecurity/247228-encryption-battle-reaches-capitol-hill

28 "Senate Judiciary Committee Holds Hearing on FBI Oversight," CQ Congressional Transcripts, December 9, 2015. http://www.cq.com/doc/congressionaltranscripts-4803506?2

29 Lauren Williams, "Yes Terrorists Use Encryption But That Doesn't Mean It's A Bad Thing," Think Progress, November 17, 2015. http://thinkprogress.org/world/2015/11/17/3722725/isis-encryption-paris-attacks/

30 Id.

31 Emma Woollacott, "MPs Slam 'Unintended Consequences' Of UK's Investigatory Powers Bill," Forbes, February 1, 2016. http://www.forbes.com/sites/emmawoollacott/2016/02/01/mps-slam-unintended-consequences-of-uks-investigatory-powers-bill/#3a2f386e47af

32 Owen Bowcott, "Investigatory powers bill: snooper's charter lacks clarity, MPs warn," The Guardian February 1, 2016. http://www.theguardian.com/law/2016/feb/01/investigatory-powers-bill-snoopers-charter-lacks-clarity-mps-warn

33 Id.

34 Jeremy Kahn, "Apple's Encryption Looks Safe as U.K. Commons Passes Spy Bill," Bloomberg Technology, June 7, 2016. http://www.bloomberg.com/news/articles/2016-06-07/apple-s-encryption-looks-safe-as-u-k-commons-passes-spy-bill.

35 Id.

36 Id.

37 Id.

38 Ellen Nakashima and Andrea Peterson, "The British want to come to America – with wiretap orders and search warrants," The Washington Post, February 4, 2016. https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

39 Id.

40 Id.

41 Id.

42 Liam Tung, "Encryption backdoors by law? France says 'non,'" ZD Net, January 18, 2016. http://www.zdnet.com/article/encryption-backdoors-by-law-france-says-non/

43 Id.

44 Phil Muncaster, "French Government Rejects Encryption Backdoors," Infosecurity Magazine, January 19, 2016. http://www.infosecurity-magazine.com/news/french-government-rejects/

45 Agence France-Presse, "French parliament votes to penalize smartphone makers over encryption," The Guardian, March 3, 2016. http://www.theguardian.com/technology/2016/mar/03/french-parliament-penalise-smartphone-makers-over-encryption

46 Id.

47 "Dutch government says no to 'encryption backdoors,'" BBC News, January 7, 2016. http://www.bbc.com/news/technology-35251429

48 Id.

49 Sara Zaske, "While US and UK governments oppose encryption, Germany promotes it. Why?" ZD Net, October 26, 2015. http://www.zdnet.com/article/while-us-and-uk-govts-oppose-encryption-germany-promotes-it-why/

50 Id.

51 Loek Essers, "No encryption back doors, says EU digital commissioner," PC World, May 20, 2015. http://www.pcworld.com/article/2924632/no-encryption-back-doors-says-eu-digital-commissioner.html

52 Id.

53 Nancy Scola, "EU digital official: Encryption backdoors a 'bad idea,'" Politico Pro, March 2016. https://www.politicopro.com/tech/whiteboard/2016/03/eu-digital-official-encryption-backdoors-a-bad-idea-068807

54 Chris Buckley, "China Passes Antiterrorism Law That Critics Fear May Overreach," The New York Times, December 27, 2015. http://www.nytimes.com/2015/12/28/world/asia/china-passes-antiterrorism-law-that-critics-fear-may-overreach.html

55 Id.

56 "India withdraws controversial encryption policy," BBC News, September 22, 2015. http://www.bbc.com/news/world-asia-india-34322118

57 "Iran orders social media sites to store data inside country," Reuters, May 29, 2016. http://www.reuters.com/article/internet-iran-idusl8n18q0in

58 Id.

59 Jeb Blount and Marcelo Teixeira, "Brazil court lifts suspension of Facebook's WhatsApp service," Reuters, December 17, 2015. http://

www.reuters.com/article/us-brazil-whatsapp-ban-idUSKBN0U000G20151217

60 Id.

61 Id.

62 Mike Murphy, "Brazil shut down WhatsApp for roughly 100 million people for 12 hours," Quartz, December 17, 2015. http://qz.com/576485/brazil-has-shut-down-whatsapp-for-roughly-100-million-people/

63 Will Connors, "Facebook Executive Arrested in Brazil," The Wall Street Journal, March 1, 2016. http://www.wsj.com/articles/facebook-executive-arrested-in-brazil-1456851506?cb=logged0.2916669365819827

64 "Facebook executive says Brazil jail stint won't slow company's growth," Reuters, March 5, 2016. https://www.theguardian.com/technology/2016/mar/05/facebook-brazil-diego-dzodan-arrest-sao-paulo

65 "UN human rights chief backs Apple in FBI encryption row," BBC News, March 4, 2016. http://www.bbc.com/news/technology-35725859

66 Id.

67 Id.

68 Bill text available at: https://lieu.house.gov/sites/lieu.house.gov/files/documents/LIEU_027_xml%20%28ENCRYPT%20Act%20of%202016%29.pdf

69 Bill text available at: https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf

70 "US Cybercom and the NSA: A Strategic Look with ADM Michael S. Rogers," The Atlantic Council, January 21, 2016. http://www.atlanticcouncil.org/events/webcasts/us-cybercom-and-the-nsa-a-strategic-look-with-adm-michael-s-rogers.

71 Bruce Schneier Berkman, Kathleen Seidel, and Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," February 11, 2016. https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf.

72 "Don't Panic: Making Progress in the 'Going Dark' Debate," Harvard University Berkman Center for Internet & Society, February 1, 2016. https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

73 Andrea Peterson, "Why the Government Can't Actually Stop Terrorists From Using Encryption," The Washington Post, March 15, 2016. https://www.washingtonpost.com/news/the-switch/wp/2016/03/15/why-the-government-cant-actually-stop-terrorists-from-using-encryption/.

74 Steven Nelson, "Encryption Backdoor Debate Centers on Catching Stupid Criminals," US News and World Report, September 21, 2015. http://www.usnews.com/news/articles/2015/09/21/encyrption-backdoor-debate-centers-on-catching-stupid-criminals.

75 Ryan Hagemann and Andrew Chang, "Encryption showdown: Burr-Feinstein vs McCaul-Warner," The Hill, April 25, 2016. http://thehill.com/blogs/congress-blog/technology/277467-encryption-showdown-burr-feinstein-vs-mccaul-warner.

76 "Answers to your questions about Apple and security," http://www.apple.com/customer-letter/answers/.

77 Hon. Newt Gingrich and Hon. Jane Harman, "A National Debate on Encryption – Now," The Hill, April 12, 2016. http://thehill.com/opinion/op-ed/276071-a-national-debate-on-encryption-now.