House Judiciary Committee &
House Energy and Commerce Committee
Encryption Working Group

Encryption Working Group
Year-End Report

December 20, 2016

Signed by:

Chairman Fred Upton (R-MI)
Ranking Member Frank Pallone, Jr. (D-NJ)
Rep. Bill Johnson (R-OH)
Rep. Yvette D. Clarke (D- NY)

Chairman Bob Goodlatte (R-VA)
Ranking Member John Conyers, Jr. (D-MI)
Rep. Darrell Issa (R-CA)
Rep. Zoe Lofgren (D-CA)
Rep. James Sensenbrenner (R-WI)
Rep. Susan DelBene (D-WA)

Introduction

On February 16, 2016, a federal magistrate judge in the U.S. District Court for the Central District of California issued an order requiring Apple, Inc. to assist the Federal Bureau of Investigation (FBI) in obtaining encrypted data off of an iPhone related to a 2015 shooting in San Bernardino, California. Apple resisted the order. This particular case was resolved when the FBI pursued a different method to access the data stored on the device. But the case, and the heated rhetoric exchanged by parties on all sides, reignited a decades-old debate about government access to encrypted data.

The law enforcement community often refers to their challenge in this context as "going dark." In essence, "going dark" refers to advancements in technology that leave law enforcement and the national security community unable to obtain certain forms of evidence. In recent years, it has become synonymous with the growing use of strong default encryption available to consumers that makes it increasingly difficult for law enforcement agencies to access both real-time communications and stored information. The FBI has been a leading critic of this trend, arguing that law enforcement may no longer be able "to access the evidence we need to prosecute crime and prevent terrorism, even with lawful authority."[1] As a result, the law enforcement community has historically advocated for legislation to "ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to keep America safe."[2]

Technology companies, civil society advocates, a number of federal agencies, and some members of the academic community argue that encryption protects hundreds of millions of people against theft, fraud, and other criminal acts. Cryptography experts and information security professionals believe that it is exceedingly difficult and impractical, if not impossible, to devise and implement a system that gives law enforcement exceptional access to encrypted data without also compromising security against hackers, industrial spies, and other malicious actors.[3] Further, requiring exceptional access to encrypted data would, by definition, prohibit some encryption design best practices, such as "forward secrecy," from being implemented.[4]

---

[1] Remarks of James B. Comey, Director, FBI, at the Brookings Institution, Washington, D.C. (Oct. 16, 2014).

[2] *Id*.

[3] *See*, *e.g*., Harold Abelson, et al., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, Computer Science and Artificial Intelligence Laboratory Technical Report, MIT-CSAIL-TR-2015-026, Massachusetts Institute of Technology, July 6, 2015.

[4] *Id.* A system that employs "forward secrecy" develops new keys for each transaction, meaning an attacker cannot access data from previous or subsequent transactions. An attacker who breaches a system that provides forward secrecy can only view data from the time of the breach until the breach is discovered and rectified. Prior data

These two outlooks are not mutually exclusive. The widespread adoption of encryption poses a real challenge to the law enforcement community *and* strong encryption is essential to both individual privacy and national security. A narrative that sets government agencies against private industry, or security interests against individual privacy, does not accurately reflect the complexity of the issue.

Recognizing the need to examine this question in a deliberate manner, the Chairmen and Ranking Members of the House Committee on Energy and Commerce and Committee on the Judiciary established a bipartisan, joint-committee working group to conduct a thorough and objective review of the encryption challenge. The Encryption Working Group (EWG) includes two Republicans and two Democrats from each Committee, as well as the Chairmen and Ranking Members of the respective Committees serving as ex officio members. The following subset of EWG members submits this report to enhance the public debate surrounding the use of encryption:

Committee on Energy and Commerce	Committee on the Judiciary
Chairman Fred Upton (R-MI)	Chairman Bob Goodlatte (R-VA)
Ranking Member Frank Pallone, Jr. (D-NJ)	Ranking Member John Conyers, Jr. (D-MI)
Rep. Bill Johnson (R-OH)	Rep. Darrell Issa (R-CA)
Rep. Yvette D. Clarke (D-NY)	Rep. Zoe Lofgren (D-CA)
	Rep. Jim Sensenbrenner (R-WI)
	Rep. Suzan DelBene (D-WA)

Over the past six months, the staff and members of the EWG, representing the respective Committees and member offices, held meetings, briefings, and roundtables with dozens of stakeholders from private industry, the intelligence community, federal law enforcement, state and local law enforcement, civil society, and the academic community.

Observations

Based on their work, the above listed members of the EWG offer four observations that may provide the foundation for further examination of this issue by the Energy and Commerce and Judiciary Committees in the next Congress.

---

remains encrypted. Additionally, under a system employing forward secrecy, session keys are destroyed after each transaction.

Observation #1: Any measure that weakens encryption works against the national interest.

To be clear, the widespread adoption of encryption has had a profound impact on the law enforcement community. Even with a lawful court order, even in dire circumstances, the authorities may not have access to encrypted data. The EWG met with representatives of federal, state, and local law enforcement, as well as with different components of the intelligence community. Each of these agencies described the challenges of obtaining encrypted data that was once commonly available to analysts and investigators.

However, stakeholders from all perspectives acknowledged the importance of encryption to our personal, economic, and national security. Representatives of the national security community told the EWG that strong encryption is vital to the national defense and to securing vital assets, such as critical infrastructure. Civil society organizations highlighted the importance of encryption for individual privacy, freedom of speech, human rights, and protection against government intrusion at home and abroad. Private sector stakeholders—in particular, their information security officers—and members of the academic community approached the question from an engineering perspective—against a wide array of threats, foreign and domestic, encryption is one of the strongest cybersecurity tools available.

Congress should not weaken this vital technology because doing so works against the national interest. However, it should not ignore and must address the legitimate concerns of the law enforcement and intelligence communities**.**

To this end, Congress should explore proposals that have so far received little attention in the committees, but may offer valuable assistance to law enforcement agencies in a digital landscape where default strong encryption is ubiquitous. These may include—but are not limited to—opportunities for collaboration between the law enforcement community and the technology sector and information sharing between different elements of the law enforcement community. Failure to examine these ideas risks further entrenchment of the status quo and limits the potential for valuable cooperation between law enforcement, the intelligence community, and private industry.

Observation #2: Encryption technology is a global technology that is widely and increasingly available around the world.

Data flows with little regard for national borders. Many of the private companies that met with the working group have a multinational presence and are subject to the laws of many different jurisdictions. Several of these companies noted a trend towards data localization requirements in foreign countries, driven at least in part by the difficulty in obtaining data for use in routine criminal investigations. Conversely, current legal authorities may be inadequate for federal agencies attempting to access data overseas.

Encryption technology is free, widely available, and often open source.[5] Law enforcement stakeholders acknowledged to the EWG that a Congressional mandate with respect to encryption—requiring companies to maintain exceptional access to data for law enforcement agencies, for example—would apply only to companies within the United States. The consequences for such a policy may be profound, but they are not likely to prevent bad actors from using encryption.

Representatives of various private companies told the EWG that a mandate compromising encryption in the U.S. technology sector would simply shift consumers to products offered by foreign companies. These forces might incentivize larger companies to leave the United States, and render small business and other innovators in the field obsolete. If a U.S.-based company moved operations to a country with a more favorable legal regime, the law enforcement and intelligence communities might lose access to everything in that company's holdings—encrypted or not.

Congressional action in this space should weigh any short-term benefits against the long-term impacts to the national interest. Congress cannot stop bad actors—at home or overseas—from adopting encryption. Therefore, the Committees should explore other strategies to address the needs of the law enforcement community.

Observation #3: The variety of stakeholders, technologies, and other factors create different and divergent challenges with respect to encryption and the "going dark" phenomenon, and therefore there is no one-size-fits-all solution to the encryption challenge.

[5] *See* Bruce Schneier, Kathleen Seidel & Saranya Vijayakumar, *A Worldwide Survey of Encryption Products*, Feb. 11, 2016.

The challenge of improving law enforcement access to encryption depends on a multitude of factors. Federal law enforcement agencies like the FBI and the United States Secret Service face obvious challenges from the growing use of strong encryption. Although federal law enforcement agencies told the EWG that they encourage the use of encryption for the protection of sensitive information—including data retained by the federal government—they cite the increased use of encryption by suspected criminals and victims of crime as a severe challenge to their public safety mission.

State and local law enforcement agencies face similar challenges, but across a wide spectrum due to massive variation in access to resources, personnel, and technical capability. Representatives from the local law enforcement community showed the EWG how encryption has hampered the investigations of even the most common crimes. Although some metropolitan police departments showed us capabilities that approach those of federal law enforcement, there is a significant overall gap between the knowledge and resources available to federal law enforcement and state and local agencies. Further, many in the law enforcement community, especially smaller agencies, expressed frustration over the challenge of navigating the processes put in place by private companies to respond to law enforcement requests for information.

Like the federal law enforcement community, the intelligence community is generally well-resourced and attracts highly skilled personnel. These advantages, and a difference in mission, often leave intelligence agencies better situated to work around the challenges posed by the widespread adoption of encryption technologies. At present, therefore, the challenge appears to be more akin to "going spotty," than "going dark" for the intelligence community. As default strong encryption becomes more prevalent in societies around the world, however, so too will the challenge for the intelligence community.

Other agencies across the federal government also have a stake in the debate. Some, like the Department of Health and Human Services, for example, generally encourage the use of encryption to secure sensitive information.[6] Others, like the Department of State, have actively encouraged the development of strong encryption in support of specific overseas and diplomatic missions.[7]

The wide array of encryption technologies also weighs against a one-size-fits-all approach to the needs of the law enforcement community. For example, although much of the

[6] 45 C.F.R. §164.312.

[7] Elias Groll, *How Hillary Clinton helped Build WhatsApp's State-of-the-Art Encryption*, FOREIGN POLICY, April 6, 2016.

debate has focused on access to data-at-rest—like the information stored on a mobile phone—the FBI relies on different techniques and legal authorities to intercept data-in-motion. An agency's ability to access encrypted information in either form will depend further on the type of encryption deployed—e.g., end-to-end encryption and a managed key architecture offer different sets of challenges to investigators. Any interaction between the private sector and law enforcement on this front will be further complicated by the nature of the product or service involved, the nature of the client—e.g., corporation, government entity, or private consumer—the business model of the company, and the security architecture employed in each specific case.

These diverse interests highlight the complexity of the encryption debate. Therefore, there is no "one-size-fits-all" answer or a "solution" to this challenge. This does not mean that nothing can be done. There is ample opportunity to achieve progress by focusing on a number of discreet issues that hinder law enforcement's ability to obtain information in light of encryption. No individual issue will address law enforcement's concerns but collectively there is opportunity to mitigate the challenge.

Observation #4: Congress should foster cooperation between the law enforcement community and technology companies.

Public perception and recent tensions notwithstanding, there is already substantial cooperation between the private sector and law enforcement. Private company stakeholders demonstrated an ability to assist federal, state, and local agencies with access to information to the extent possible and with service of a lawful order, and expressed a willingness to explore ways to improve and enhance that collaboration.

Stakeholders from all sides were nearly unanimous in describing a significant gap in the technical knowledge and capabilities of the law enforcement community, particularly at the state and local levels. This results in a range of negative consequences that not only hinder law enforcement's ability to pursue investigations but also contribute to its tension with the technology community. For example, from the perspective of law enforcement, routine requests for data are often challenged by the companies, unnecessarily delayed, or simply go unanswered. From the perspective of the companies, these requests often lack appropriate legal process, are technically deficient, or are directed to the wrong company altogether.

It also remains unclear whether the law enforcement community is positioned to fully leverage the unencrypted information still held by many companies. A number of stakeholders acknowledged the potential benefit of improving law enforcement's understanding of what data or information is available, who controls it, and how it could be useful to investigators. In

particular, companies are often able to provide volumes of unencrypted metadata associated with their products or services. In some cases, this source of information could be useful to investigators. In others, one representative of a law enforcement agency told the EWG, access to a stream of metadata might be more like "looking for a particular grain of sand on the beach."

Congress can play an important role in encouraging or facilitating opportunities to strengthen and expand collaboration between the technology sector and law enforcement. Fostering such cooperation would not only help strengthen law enforcement's capabilities, it would also assist in enhancing communication and lessening distrust between the two sides.

These and similar challenges can be mitigated by exploring opportunities to reduce the knowledge and capabilities gap between law enforcement and the technology community. This effort will not only improve law enforcement's effectiveness but also has the potential to reduce friction with the technology community while also exploring and addressing civil liberties concerns.

Next Steps

Based on these observations, the members of the EWG listed above have identified the following areas for future discussion by the Committee on Energy and Commerce and the Committee on the Judiciary. These suggestions are not exhaustive, and are intended provide starting points for the Committees' work in this space in the next Congress, without precluding or undermining consideration of related issues as they emerge or evolve.[8]

Law Enforcement Requests for Information

Congress should explore means of providing assistance to law enforcement agencies with respect to navigating the process of accessing information from private companies. A few relatively uncontroversial ideas could radically improve the ability of the law enforcement community to operate in a digital environment—and also reduce tensions between law enforcement and private industry. These ideas include, but are not limited to:

- Exploring tools that might help companies clarify what information is already available to law enforcement officers, and under what circumstances.

- Examining federal warrant procedures to determine whether they can be made more efficient, consistent with current constitutional standards.

- Examining federal warrant procedures to ensure that they are clear and consistent with respect to law enforcement access to digital information.

- Examining how law enforcement can better utilize existing investigative tools.

- Authorizing and modernizing the National Domestic Communications Assistance Center (NDCAC). The NDCAC, organized under the Department of Justice, is a hub for

[8] There are many interesting aspects of this evolving landscape—such as prospect of quantum computing—that have the potential to influence future policy decisions. Likewise, other ongoing projects, including a study recently launched by the National Academies to examine options and trade-offs for obtaining access to encrypted data. As noted in the project summary, the "study will not seek to answer the question of whether access mechanisms should be required but rather will provide an authoritative analysis of options and tradeoffs." (*See, e.g.* http://www8.nationalacademies.org/cp/projectview.aspx?key=49806) This study, and similar efforts, will further inform the Committees examination of this issue.

technical knowledge management designed to facilitate information sharing among law enforcement agencies and the communications industry. NDCAC does not have an investigative role and is not responsible for execution of electronic surveillance court orders. Congress has never formally authorized the NDCAC, but its current structure seems conducive to providing the law enforcement community a forum through which to share information and benefit from existing technical expertise.

Metadata Analysis

As more and more of our daily lives are connected to the internet, our digital "footprints" grow through the production of metadata. Some argue that effective analysis of this metadata would help investigators offset the loss of encrypted content. Some representatives of the law enforcement community were hesitant to adopt this view. They acknowledged that metadata can be helpful in certain circumstances but also argued that it is frequently challenging for law enforcement agencies to make sense of large amounts of metadata. Law enforcement stakeholders also noted that metadata may be a poor replacement for content in court. For example, a record of the time and place from which a text message was sent might be less persuasive to a jury than the text message itself.

Metadata may not completely replace the loss of encrypted content, but metadata analysis could play a role in filling in the gap. The technology community leverages this information every day to improve services and target advertisements. There appears to be an opportunity for law enforcement to better leverage this information in criminal investigations. Acknowledging that metadata cannot replace encrypted content in all cases, the value of this data should be explored. Questions in this area might include:

- When is law enforcement able to access certain types of metadata, what kind of metadata can they access, and from whom do they obtain this data?
- What privacy interests are implicated when law enforcement analyzes large amounts of metadata over time?
- What kind of algorithmic or other technical tools would law enforcement agencies need in order to fully leverage this data?
- What judicial and evidentiary processes around metadata currently exist, and do they limit its effectiveness or applicability in court?

- What knowledge, resource, or technical impediments exist to limit the ability of law enforcement agencies, especially at the state and local level, to more effectively leverage this information?

Legal Hacking

Legal hacking, also known as lawful hacking, is an investigative tactic whereby a law enforcement agency exploits a vulnerability in the digital security of a device or service in order to obtain evidence of a crime. Many stakeholders argue that, rather than building new vulnerabilities into secure products to facilitate law enforcement access, law enforcement agencies should be given the resources to exploit the flaws in secure products that already exist. Several law enforcement agencies noted that legal hacking is a time- and resource-intensive approach, and limited to the subset of cases where the agency actually knows of a flaw to exploit. These concerns are amplified at the state and local level, where resources and technical capabilities may be even scarcer. Other stakeholders expressed concern that a legal hacking regime creates the wrong incentives for government agencies that should be working with private companies to patch vulnerabilities and improve cybersecurity.

In the next Congress, the Committees might explore a legal framework under which law enforcement agencies can exploit existing flaws in digital products. Questions in this area include, but are not limited to:

- What sort of legal process, if any, is required in order to authorize a law enforcement agency to "hack?"

- Should a law enforcement agency disclose vulnerabilities leveraged in legal hacking to the affected companies, and if so, when?

- Is the current Administration's Vulnerabilities Equities Process—the ad hoc process through which the federal government currently determines whether or not to disclose vulnerabilities already in its possession—adequate? Should Congress provide guidance or authorize some formal structure for the process?

- How do the challenges faced by the law enforcement community differ from those of the intelligence community, and how are the different equities of different agencies balanced in the Vulnerabilities Equities Process?

- Does legal hacking "scale," particularly when evaluating whether to provide additional resources to state and local law enforcement? Given the cost and resource-intensive nature of legal hacking, can the law enforcement community make regular use of legal hacking as an investigative technique? If so, does regular use of legal hacking raise security concerns?

Compelled Disclosure by Individuals

Although much of the debate has focused on requiring third party companies to decrypt information for the government, an alternative approach might involve compelling decryption by the individual consumers of these products. On a case-by-case basis, with proper court process, requiring an individual to provide a passcode or thumbprint to unlock a device could assist law enforcement in obtaining critical evidence without undermining the security or privacy of the broader population.

Given evolving technologies and the trend towards using biometrics—like a fingerprint or facial recognition software—to decrypt data, Congress might consider the following questions:

- Can the government compel an individual to unlock his phone without violating the protection against self-incrimination guaranteed by the Fifth Amendment to the U.S. Constitution?

- With respect to the Fifth Amendment, is there a substantive or legal difference between unlocking a device with a passcode and unlocking the device with a biometric identifier? Is entering a passcode a "testimonial act," as some courts have held? Is a fingerprint different in any way?

- What is the proper legal standard for compelling an individual to unlock a device?

- Are there other circumstances that would enable the government to compel production of a passcode without undermining the Fifth Amendment?

Privacy and Data Security

The increasing use of encryption—especially in consumer products—can be attributed, at least in part, to heightened consumer awareness and interest in online privacy and data security. Because consumers also demand the convenience and features enabled by information-sharing

and third-party access to personal information, many applications now have access to expansive consumer information. Congress should further explore the role of encryption in fostering greater data security and privacy. Relevant questions might include the following:

- Should the federal government take additional steps to address greater security around private data?
- How can companies use encryption to better protect consumers' privacy and the security of consumers' information?
- How can the government use encryption to better protect privacy and the security of information held by various agencies?
- What vulnerabilities remain after communications have been encrypted and how might those vulnerabilities be addressed?
- How would consumers' privacy and data security suffer if encryption were weakened?
- What additional tools, if any, could private companies use to secure consumers' information?

* * *

The debate about government access to encrypted data is not new—but circumstances have changed, and so too must our approach.

Encryption is inexorably tied to our national interests. It is a safeguard for our personal secrets and economic prosperity. It helps to prevent crime and protect national security. The widespread use of encryption technologies also complicates the missions of the law enforcement and intelligence communities. As described in this report, those complications cannot be ignored. This is the reality of modern society. We must strive to find common ground in our collective responsibility: to prevent crime, protect national security, and provide the best possible conditions for peace and prosperity.

That is why this can no longer be an isolated or binary debate. There is no "us versus them," or "pro-encryption versus law enforcement." This conversation implicates everyone and everything that depends on connected technologies—including our law enforcement and intelligence communities. This is a complex challenge that will take time, patience, and cooperation to resolve. The potential consequences of inaction—or overreaction—are too important to allow historical or ideological perspectives to stand in the way of progress.