GOING DARK: THE ETHICAL CHALLENGES WITH THE FBI'S GOING DARK INITIATIVE

Adam Johnson

Abstract

One of the fundamental ethical conflicts faced by the modern intelligence community is the conflict between national security and individual privacy. Recently, the FBI proposed its "Going Dark" initiative, which pushed to give law enforcement new capabilities to access private encrypted data in order to thwart terrorist attacks. This study looks at the history of laws that regulate how the government can monitor private communicate and the challenged posed by modern communication. It evaluates the ethical challenges faced by the "Going Dark" initiative and finds that it threatens both individual privacy and could expose private users to exploitation. This study concludes by offering two alternative policies that could accomplish a similar goal with less impact on the rights of Americans.

Introduction

Since its founding, the United States intelligence community has attempted to provide for the national security of our country by intercepting and interpreting the communications of potentially harmful actors. Unfortunately, some of these attempts on behalf of the intelligence community have at times challenged the civil liberties of Americans. As a result, the United States has been locked in a difficult debate regarding where the line ought to be drawn between national security and personal liberties. Today, the United States government finds itself in a similar situation with the proposition of the FBI's "Going Dark" initiative. At first glance, the FBI's initiative appears quite persuasive—extend the legal parameters of U.S. communications surveillance law to stymie the threat of terrorism and further uphold the national security of the United States. However, when analyzed in detail, the proposed initiative also appears to contain a variety of ethical challenges. These ethical challenges include: (1) the negative ramifications for private communication companies, (2) the potential increase in the domestic terrorism threat, (3) international exploitation, and (4) the possibility for abuse. Given the ethical challenges associated with the "Going Dark" initiative, U.S. policymakers face a difficult decision between further promoting the national security of the United States and upholding American civil liberties.

Background: The Government's Monitoring of Communication

The debate over where the line ought to be drawn regarding the monitoring and collection of data from electronic communications is not a new phenomenon. For decades, Congress has passed various bills defining the boundaries of communications surveillance. In order to understand the current ethical challenges associated with the government's attempts to use communication providers to intercept information for counterterrorism purposes, it is important to understand previous legal precedent regarding government wiretapping and communications surveillance. This section will cover some of the key legislative acts that define the limitations on communications surveillance over the past several decades.

The first notable act which established strict guidelines for government surveillance through wiretapping was Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Congress passed Title III in response to several congressional investigations (U.S. Department of Justice, 2013b). These investigations discovered that government agencies had conducted extensive wiretapping without receiving proper legal authorization. Specifically, Title III regulated government technical surveillance in three distinct ways. First, the act prohibited government agencies from intercepting either wire or oral communications without legal authorization.

Second, Title III established procedures for government agencies to obtain warrants in order to wiretap identified targets. Finally, Title III regulated how law enforcement could disclose and use the information collected via wiretapping (U.S. Department of Justice, 2013b). The Title III regulations were consistent with previous legal precedent established by the Supreme Court. In *Berger v. New York*, the Supreme Court concluded that the Fourth Amendment's protection against unreasonable searches and seizures extended to the interception of communication where individuals have a reasonable expectation of privacy (U.S. Department of Justice, 2013b). Originally, Title III only covered wiretapping of wire and oral communication. However, the regulations within Title III were significantly revised following the passing of the Electronic Communication Privacy Act of 1986.

The Electronic Communication Privacy Act (ECPA) further clarifies the regulations of government wiretapping found under Title III of the Omnibus Crime Control and Safe Streets Act (U.S. Department of Justice, 2013b). This act was implemented due to recent technological advancements that took place in the 1980s. For the first time, Congress had to determine how the right to privacy could be applied to new forms of communication such as email, wireless telephone conversations, and conversation data stored on computers. Modern means of communication presented new challenges in the ongoing debate over where to draw the line between personal privacy and national security. In practice, the act extended the regulations regarding the interception of conversations taking place on hard telephone lines to also include information being shared and stored on personal computers. The act further regulated the government's electronic surveillance of emails, telephone conversations, and data stored electronically (U.S. Department of Justice, 2013b).

Advances in online communication increased the amount of online communication data that could be tapped by the United States government. As these advancements in communication developed, it was determined that some forms of online communication were protected and required a warrant to seize the information via wiretapping. However, certain laws allowed the government to seize stored information that was shared through means of online communication without a warrant. Title II of the ECPA, known as the Stored Communications Act, granted the U.S. government the ability to access various kinds of stored communications without first obtaining a warrant ("Electronic Communications," n.d.). The following table illustrates which collection actions by the United States government require a warrant ("Electronic Communications," n.d.).

Type of Communication	Required for Law Enforcement Access	Statute
Email in transit	Warrant	Electronic Communications Privacy Act of 1986
Email in storage on home computer	Warrant	4th Amendment of the U.S. Constitution
Email in remote storage, opened	Subpoena	Stored Communications Act
Email in remote storage, unopened for 180 days or less	Warrant	Stored Communications Act
Email in remote storage, unopened for more than 180 days	Subpoena	Stored Communications Act

Figure 1. Graph of change in commodity outlays by program 1978-2014 (Zulauf & Orden, 2016).

In addition to regulating email monitoring and data collection, Title II of the ECPA empowers the U.S. government to collect data and information records from communications providers. Under this statute, the government can compel any communications provider, through the use of a National Security Letter (NSL) or court order, to disclose their records on a given customer (Doyle, 2012). Specifically, an NSL can be used to obtain the name, address, length of time, location of telephone connection (local or long distance), telephone number, network address, and means of payment for communication services from a communications provider on any given customer targeted by the United States government ("Electronic Communications," n.d.). Any other non-content related customer records can only be obtained through a court order.

In 1994, the ECPA was amended by the Communications Assistance for Law Enforcement Act (CALEA) which enhanced law enforcement's ability to legally intercept or acquire data from telecommunication devices and carriers. CALEA's origins stem from concerns voiced by Federal Bureau of Investigation (FBI) in the mid-1990's. In short, the FBI grew concerned that increased use of cellular phones would make the process of monitoring cellular networks of private phone companies slower and nearly impossible to execute in some cases (Kopel, 1998). The goal of CALEA was to increase the effectiveness and efficiency of law enforcement electronic surveillance (Figliola, 2007). The Congressional Research Service best defined CALEA's goal: "CALEA is intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently, despite the deployment of new digital technologies and wireless services by the telecommunications

industry" (Figliola, 2007, p. 1). In order to achieve this goal, CALEA promulgated that telecommunications carriers assist law enforcement in performing electronic surveillance on their digital networks. Specifically, CALEA ordered that telecommunication industries design and implement certain surveillance assistance capabilities in their networks that would support law enforcement's conduct of legal electronic communication surveillance. As a result of CALEA, telecommunications companies were required to have the following capabilities: (1) isolation of all wire and electronic communications of a target transmitted by the carrier within a given service area, (2) isolation of call-identifying information in regards to the targeted communication, (3) the ability to provide intercepted communications and call-identity information to law enforcement upon a legal request, and (4) the ability to intercept a targeted communication unobtrusively so that targets are not made aware of the surveillance of their electronic communications (Figliola, 2007). In order to uphold and protect the privacy rights of individuals, CALEA also required that a court order be presented to any telecommunications company before law enforcement could acquire the collected electronic communication data (Figliola, 2007).

The policies regarding government surveillance within CALEA were not initially well-received by the general public. Many Americans concluded that the surveillance capabilities granted by the CALEA statute went too far and threatened individual privacy. Even certain members of the Supreme Court worried that the provisions within CALEA threatened the fundamental right to privacy enshrined in the Fourth Amendment of the Constitution. Justice Thurgood Marshall took issue with the statute when he stated that, "Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts" (Kopel, 1998, para. 4). Americans were clearly concerned about how far the government would take its new technical surveillance capabilities. The implementation of CALEA and the backlash it received from members of government and the American public further exemplify the ethical difficulty in determining the proper balance between government surveillance and personal privacy.

Following the terror attacks of September 11th, the United States Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act). The Patriot Act was a direct response to the heightened terrorism threat in the early 2000's. As a result, the Act amended various aspects of United States law which dealt with the investigation and prosecution of terrorism. In regards to the monitoring of technical communication, the Patriot Act had one notable impact.

The Patriot Act significantly expanded the predicates for intercepting and

collecting technical communications ("Sunset Provisions," 2005). Specifically, Section 201 of the USA Patriot Act expanded the provisions within Title III regarding the interception of communication to include the legal wiretapping of crimes relating to counterintelligence and terrorism ("Director Discusses Encryption," 2005). In essence, Section 201 of the USA Patriot Act brought federal wiretap statutes (such as the ones in ECPA) into the 21st century. Preceding the implementation of the Act, federal law enforcement was unable to legally monitor, collect, or obtain communications data that pertained to any form of terrorist activity ("Sunset Provisions," 2005). Such legal precedent created a significant gap between government surveillance and national security. Due to such legal practices, intelligence and investigative agencies, such as the FBI, operated largely in the dark when it came to detecting and exploiting crimes pertaining to terror. It was not until Section 201 of the Patriot Act that this gap in intelligence was closed and intelligence agencies were granted the legal capabilities to monitor and investigate the full range of crimes related to terrorism ("Sunset Provisions," 2005).

To date, there is still a political debate regarding the legality of the provisions within the Patriot Act. When it was originally passed in 2001, just one senator voted against the act on the grounds that it significantly violated the civil liberties of Americans. However, in 2015, 77 United States senators voted to modify various aspects of the Patriot Act by implementing a new law titled the USA Freedom Act (Baker, 2015). Specifically, the USA Freedom Act restored several provisions within the USA Patriot Act while simultaneously revoking others. One of the most prominent provisions revoked by the Freedom Act was Section 215 of the Patriot Act, which granted the National Security Agency the capability to collect large amounts of communication metadata (bulk collection) within the United States. Furthermore, the Freedom Act mandated stricter requirements for intelligence agencies seeking to obtain communication data and transactions from private communication providers (Volz, 2015). Despite these regulating provisions within the Act, U.S. intelligence agencies still attempted to push the bounds of the current legal practices regarding communication surveillance.

Following the passage of the Freedom Act of 2015, the FBI attempted to extend the bounds of its communications interception capabilities. According to the FBI, modern forms of communication, specifically encrypted forms, presented new challenges to the FBI's current technological surveillance capabilities and methods. As a result, the FBI called for an amending of the Communications Assistance for Law Enforcement Act (CALEA) to include new provisions granting them the ability to penetrate the encrypted servers of private communication companies ("Going Dark," n.d.).

There is still much debate over the necessity and legality of the FBI's demands. Private communication companies and various political officials argue that the

demands of the FBI are unwarranted (Gross, 2015). Conversely, U.S. intelligence agencies, namely the FBI, have asserted that if adequate adjustments are not made to current U.S. technological surveillance procedures, national security will be in jeopardy ("Going Dark," n.d.).

Research and Analysis

Challenges Presented by Modern Forms of Communication

Recent advancements in end-to-end encrypted communication have created a new system of communication that is significantly more difficult to surveil. Due to the leaks produced by Edward Snowden regarding the NSA's mass surveillance of transmitted communication data, several tech companies have taken a more public role in pushing back against the U.S. government's encroachment of personal privacy (Brown & Perez, 2014). In September 2014, Apple was one of the first communications companies to program their new operating system, IOS 8, with advanced forms of data encryption. According to their privacy policy, Apple specified that personal data stored and transmitted on communication devices running the IOS 8 software were protected by the user's private security passcode. Furthermore, Apple's privacy policy stressed that due to the unique user passcode encryption on each device, it was not "technically feasible" for Apple to respond to government warrants calling for the extrapolation of data from a targeted user's communication device (Finklea, 2016, p. 5). Along similar lines, Apple has also clarified that "there's no way for us to decrypt your data when it's in transit between devices" (Apple Inc., n.d., para. 5). As a result of Apple's inability to scan or decrypt a customer's communication data, the company concluded that it would be unable to comply with any wiretap court order (Yadron, 2016).

Similar to Apple, Google has also implemented new encryption technology in its communications systems. In November 2014, Google launched its Android 5.0 operating system which contained default privacy protection settings that automatically encrypted communication data with a secure user password. Moreover, data transmitted on any communication device running Android 5.0 is automatically encrypted with a passcode and can only be recovered when a valid passcode is entered. What makes investigative matters difficult for law enforcement is that Google, similarly to Apple, does not have the passcode to any of the communication data encrypted on their servers (Finklea, 2016). Thus, wiretap orders prove to be considerably difficult to implement on devices running Android 5.0 software.

The recent breakthroughs in communication encryption have significantly hindered a variety of national security surveillance operations and investigations.

In the realm of law enforcement, safety officials have equated the new developments in communication encryption to "a house that can't be searched, or a car trunk that could never be opened" (Finklea, 2016, p. 6). Currently, communication companies such as Apple and Google are not required under federal law to possess a key to their encryptions. As a result, a significant portion of communication data transmitted through the servers of these companies may not be readily available to law enforcement upon an official request via a court order (Finklea, 2016). As the law stands (specifically in regards to CALEA), telecommunications companies providing broadband internet and VoIP services must be capable of readily assisting law enforcement in the monitoring and collecting of real time communication data. For companies such as Apple and Google, the requirements within CALEA are not applicable to their communication infrastructures. Specifically, Apple's text messaging system iMessage is not transmitted through broadband or VoIP providers. Therefore, communications taking place within the iMessage system fall outside the legal scope of CALEA (Finklea, 2016). Given the current status of the law, communication companies such as Apple and Google have successfully stymied U.S. law enforcement's attempts to collect and analyze real time or near real time communication data within their encrypted systems. According to U.S. intelligence agencies, the status quo regarding the conflict between wiretapping and encrypted communication poses a significant threat to United States national security (Homeland Security Committee, 2016). As a result of this determined threat, the FBI through their "Going Dark" initiative has attempted to reform the current mandates within CALEA to better address the gaps between electronic surveillance and encrypted communication.

The FBI's "Going Dark" Initiative

The FBI's "Going Dark" initiative is a recent attempt to extend the requirements mandated in CALEA to require internet based communication providers such as Google, Facebook, Twitter, Skype, and Blackberry, to reprogram their encryptions within their communication systems to have a backdoor for legal wiretapping. The term "Going Dark" refers to a phenomenon where criminals use encrypted communication to evade being detected by law enforcement (Homeland Security Committee, 2016). The threat of criminals going dark was always of concern to the United States intelligence community. In 2015, the concerns surrounding encryption communication surged following the terrorist attacks in Paris and San Bernardino where it was determined that the attackers used encrypted forms of communication to avoid identification.

Today, an increasing number of criminals and terrorists operate in the dark by using end-to-end encryption to conceal their activities, communications, photographs, and records (Homeland Security Committee, 2016). As a result of

the increasing use of encrypted communication, intelligence officials and law enforcement have stated that their ability to gain access to the digital communications of terrorists and criminals has been significantly hindered. Previous FBI Director James Comey testified before the Senate Judiciary Committee that "[t]here 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" (Homeland Security Committee, 2016, p. 12). Encryption communication is becoming one of the primary forms of communication for criminals and terrorist organizations. In 2015 alone, it was determined that the perpetrators behind the terrorist attacks in Texas, France, and San Bernardino all utilized various forms of encrypted communication (Homeland Security Committee, 2016).

The U.S. intelligence community faces two distinct challenges when it comes to monitoring and exploiting information from encrypted terrorist communications. The first challenge is monitoring, intercepting, and obtaining real-time communications data which is in motion. Data in motion includes real-time communication being transmitted from phone calls, emails, text messages, and chat sessions ("Going Dark," n.d.). The second challenge concerns monitoring and collecting "data at rest" from encrypted communication devices ("Going Dark," n.d., para. 2). The term "data at rest" refers to data that is stored on encrypted communication devices such as saved emails, text messages, photos, and videos ("Going Dark," n.d., para. 2). Both of these forms of data significantly contribute to detecting, identifying, and exploiting terrorist operations in the United States and abroad. However, current practices regarding court orders and warrants have made it increasingly difficult for law enforcement to obtain stored and real-time data transmitted through encrypted communication servers. As a result of the status quo regarding court orders and warrants, law enforcement's ability to quickly obtain valuable information that could identify terror suspects is rapidly eroding ("Going Dark," n.d.).

In an effort to respond to their eroding capabilities, the FBI has recently attempted to expand the reach of CALEA to cover encrypted forms of communication. Originally, CALEA mandated that all phone companies conform to wiretap standards for real-time surveillance. In 2005, CALEA was extended to also cover broadband service providers (such as ISPs and colleges). Today, forms of encrypted online communication services such as Google Chat, Skype, Facebook, and Blackberry, are not covered by the provisions stated within CALEA (Kravets, 2012). Due to the present state of CALEA, these communication services listed above are not required to conform to wiretap standards that would improve the effectiveness of law enforcement's technical communication surveillance. Furthermore, by not

having to comply with current wiretapping standards, these service providers are often unable to comply with law enforcement surveillance requests when presented with a court order or warrant (Savage, 2011).

Due to the increasing use of encrypted communication by various criminal enterprises, the FBI, along with other federal agencies, has concluded that monitoring encrypted communication is a necessary aspect of United States national security. Previous FBI Director James Comey captured this assessment best when he stated, "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…we believe [going dark] must be addressed given the resulting risks are grave both in traditional criminal matters as well as in national security matters" (Homeland Security Committee, 2016, p. 10). Government and law enforcement officials are deeply concerned with the present state of U.S. national security. Without the ability to monitor these new forms of communication, officials fear that they may be less able to prevent, investigate, and prosecute criminal activities such as terrorism (Olsen, Schneier, & Zittrain, 2016). The proposed solution for fixing this technological problem surrounding the wiretapping of encrypted forms of communication is to mandate that communication companies must maintain and provide law enforcement access to their encrypted communication servers.

Ethical Challenges Associated With the Going Dark Initiative

The mandates within the FBI's "Going Dark" initiative have the potential to generate a host of ethical challenges. On its face, the FBI's initiative appears quite persuasive—extend the legal parameters of CALEA to stymie the threat of terrorism and increase the national security of the United States. However, when analyzed in detail, such a proposition appears to also contain a variety of ethical dilemmas. Specifically, this study identifies four ethical challenges associated with the "Going Dark" initiative: (1) the negative ramifications for private communication companies, (2) the potential increase in the domestic terrorism threat, (3) international exploitation, and (4) the possibility for abuse.

The first ethical challenge to consider when examining the FBI's "Going Dark" initiative is the potential negative ramifications it could have on private communication companies. Currently, companies such as Apple and Google use their encrypted servers to not only conceal the interests of their customers, but also to protect their infrastructure from outside threats such as foreign governments, international competitors, and hackers.

Moreover, encryption also protects the financial transactions and personal information of all customers utilizing the servers of one of these companies ("Going Dark," n.d.). Forcing communication companies to weaken their encrypted servers by creating a backdoor for law enforcement to exploit (which is the current goal of

the "Going Dark" initiative) makes companies more vulnerable to outside threats such as hackers and identity thieves (Udry, 2015). Several lawmakers who testified before the House of Representatives' Oversight and Government Reform Committee stated that it was "impossible" for communications companies to build backdoors in their encryptions and still keep cybercriminals out of their servers (Gross, 2015, para. 2). The ethical challenge with the "Going Dark" initiative is essentially the fact that the government would be forcing communications companies to lower the level of security currently protecting the information of billions of consumers. Moreover, if companies were forced to create a backdoor in their encrypted servers, all of the corporate information and personal data of the company's customer basis would be at an increased risk of exploitation.

In addition to potentially damaging the technical infrastructures of communication companies, the "Going Dark" initiative also risks harming the financial stability of several U.S tech giants. In today's communications market, Apple and Google place a strong emphasis on the safety and security of their encrypted servers. This is mostly due to the vast customer base of both companies. In 2016, it was estimated that Apple had more than 1 billion IOS users worldwide (Statt, 2016). Similarly in 2017, Google announced that it had over 2 billion devices actively running on its Android server (Popper, 2017). The extensive consumer size of both companies results in a network where literally billions of individuals' financial records, credit card data, identifying information, passwords, email logins, social media account information, etc. are stored at any given time. As a result of this massive amount of private information, it is essential for communication companies to develop a system where that information is secure and protected from outside threats such as identity thieves and hackers. However, by creating a backdoor, the possibility of such outside threats gaining access to these encrypted networks severely increases. This in turn could drastically impact the customer base and revenue stream of communication companies such as Apple and Google. Apple CEO, Tim Cook, highlighted this potential fear when he stated, "The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers" (Price, 2016, para. 22).

In addition to the local customer, the "Going Dark" initiative could also impact Google and Apple's foreign customer bases. According to Jon Potter, president of the Application Developers Alliance, "U.S. smartphone apps that allow back doors would likely be banned in many European countries," further impacting the financial earnings of Apple and Google (Gross, 2015, para. 12).

The stark contrast between the infrastructural stability of private companies and the capabilities of communication surveillance is an ethical dilemma that policy makers have to wrestle with when determining the future of the FBI's "Going Dark"

initiative. Backdoors in encryptions are essentially holes in security that can be exploited by both law enforcement and cybercriminals. In a sense, U.S. lawmakers are caught in between two ethical challenges when determining the future of the "Going Dark" initiative. One the one hand, the implementation of the "Going Dark" initiative means increased access to communications data for law enforcement paired with a greater vulnerability to cybercriminals. On the other, not implementing the "Going Dark" initiative likely results in increased security within communication company servers paired with greater obstructions to law enforcement investigations (Finklea, 2016).

The second ethical challenge associated with the "Going Dark" initiative is the potential for an increase in domestic terrorism due to the obstruction of communication surveillance caused by encryption. As stated previously, encrypted forms of communication present a variety of challenges to law enforcement when attempting to surveil or collect data on the communications being transmitted. Due to the surveillance difficulties associated with encrypted communication, various criminal enterprises and terrorist organizations have begun to exploit such means of communication. James Comey recently reported that terrorist organizations such as the Islamic State have started to recruit and radicalize Americans through the use of encrypted mobile messaging (Olsen et al., 2016). Such practices pose a direct threat to the national security of America. Specifically, the use of encrypted communication between the Islamic State and Americans means the FBI largely cannot collect or analyze the communication data to determine who the point of contact for the Islamic State is within the United States. As a result of this obstruction, multiple Islamic State affiliates living within the United States go unidentified and, in some cases, launch terrorist attacks such as the one in San Bernardino, California (Thomas, 2015). The ethical challenge is that if nothing is done to solve for the obstructions to terror investigations caused by encrypted communication, the national security of the United States could be placed in greater jeopardy.

The third ethical challenge stemming from the proposed "Going Dark" strategy is the potential for foreign government exploitation. Specifically, the FBI's demands for a backdoor to be programmed into the encrypted servers of Apple and Google gives authoritarian powers such as China and Russia the ability to force the same companies to produce similar keys to their encryptions (Timm, 2015). In greater detail, the government of China has recently adopted a new counterterrorism strategy which has the potential to require American communication/technology companies (such as Apple and Google) to turn over its encryption keys and program backdoors into their encrypted servers (Pierson, 2016). Unfortunately for American companies, the trajectory of Chinese cybersecurity and counterterrorism programs only seems to be heading towards a more restrictive destination. Based on the recent programs implemented by the Chinese government, especially in terms of their

recent 2015 counterterrorism law, it is clear that one of the focuses of the current administration is to strictly regulate "untrustworthy" foreign technology companies. International law firms studying the newly enacted Chinese counterterrorism law have started to warn American technology companies that China has the capability to legally demand source codes, encryption keys, and other crucial forms of information regarding communication servers from foreign technology companies currently operating in China (Alsabah, 2017).

Essentially, the ethical challenge associated with the "Going Dark" strategy is that it provides precedent for foreign nations, such as China, to enforce their laws requiring foreign communication companies to hand over their encryption keys. Currently, the only significant factor holding China back from fully implementing the laws within its new counterterrorism strategy is United States opposition. In 2015, then U.S. President, Barack Obama, articulated that his administration was very concerned with China's new counterterrorism strategy. Specifically, he stated, "This is something that I've raised directly with President Xi. We have made it very clear to them that [their requirements within their counterterrorism strategy are] something they are going to have to change if they are to do business with the United States" (Mason, 2015, para. 3). Despite the United States' strong stance on China's counterterrorism laws, it is highly likely that the Chinese government would disregard U.S. opposition if the demands within the FBI's "Going Dark" initiative were met. This is because the United States would have established a legal precedent demonstrating that it is acceptable for a government to require American communication companies to program a backdoor into their encrypted servers.

The fourth and final ethical challenge associated with the FBI's "Going Dark" initiative is the possibility for the United States government to abuse the surveillance powers and capabilities granted to them by the initiative. In 2013, the Guardian newspaper reported on one of the greatest abuses of power that has ever taken place within the U.S. intelligence community. Specifically, the newspaper reported that the National Security Agency (NSA) was collecting the phone records of millions of American citizens through an online communication surveillance program called PRISM ("Edward Snowden," 2014). After the intelligence leak, Americans quickly demanded that lawmakers hold the NSA accountable for violating the civil liberties of millions of American citizens. The NSA's PRISM program is a notable example of where the U.S. intelligence community expanded beyond the powers bestowed upon them. While there is significant contrast between the capabilities of the NSA's PRISM surveillance program and the FBI's "Going Dark" initiative, there is still an equal level of concern for abuse.

If the FBI's "Going Dark" strategy were implemented, the Bureau would have access to billions of phone records and transmitted communications data. While

such capabilities can be utilized for countering terrorism and upholding national security within the United States, such power could also be abused. Thus, if the United States implemented the policies within the "Going Dark" initiative, U.S. policymakers would have to prevent the abuse of American civil liberties. Past precedent with the NSA shows it is obvious that U.S. intelligence agencies have the ability to overstep their bounds. Thus, when considering the implementation of the "Going Dark" initiative, the United States government must also consider the ethical challenges associated with enacting the initiative.

Alternative Solutions

Given the pivotal role encryption plays in the modern investigation and counterterrorism process, it is important to construct alternative solutions to the current problem facing law enforcement and the FBI. Moreover, it would be wise for U.S. policymakers to consider several viable solutions to the current crisis. Technology experts have identified two potential alternatives to the FBI's "Going Dark" strategy that may better solve the going dark problem as well as protect the civil liberties of Americans. Specifically, these two alternative options are (1) lawful government hacking and (2) the development of a nationwide law enforcement decryption program.

The first alternative solution to the "Going Dark" initiative is the implementation of lawful hacking for official law enforcement use. In detail, law enforcement agencies could exploit already existing-security flaws in encrypted servers to obtain targeted communication data (Segal & Grigsby, 2016). Currently, such a capability is not warranted under United States law. However, Congress does have the authority to approve new legislation that would grant law enforcement the capability to hack an encrypted server with a court order. According to several technology experts who were interviewed by the Los Angeles Times, lawful hacking is a viable alternative to creating backdoors in encryption (Segal & Grigsby, 2016). Moreover, it would likely produce the same results as backdoors in encryptions without threatening the security of the encrypted server.

The second alternative to the "Going Dark" initiative is the development of a nationwide law enforcement decryption program. Currently, the challenges of going dark most significantly impact state and local law enforcement. This is mostly because both state and local law enforcement lack the resources and technical capabilities to unlock encrypted forms of communication. As a result, the executive branch should construct a national decryption program housed within the FBI. Such a program would assist state and local law enforcement when encrypted servers and communications data obstruct the investigation (Segal & Grigsby, 2016). While such a program may lead to difficulty in obtaining information from encrypted servers, a national decryption program would ultimately prove beneficial for assisting law

enforcement in investigations involving encryption.

Conclusion

Encrypted communication plays a vital role in both the world of private companies and law enforcement. Currently, law enforcement faces legitimate challenges when it encounters encrypted forms of communication during an investigation. In various situations, encryption has restricted law enforcement's ability to successfully attain information, identify targets, and prosecute criminal cases ("Going Dark," n.d.). In the state of New York alone, local law enforcement estimated that encrypted forms of communication hindered the investigations of over 175 cases between September 2014 and March 2016 ("Going Dark," n.d.). The debate between encrypted communication and national security is not an issue that will disappear in the near future. The House Homeland Security Committee captured the overall essence of this debate best when it wrote:

> 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."…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. (2016, p. 6)

There are various ethical challenges on both sides of the debate regarding the implementation of the FBI's "Going Dark" initiative. As previously noted, U.S. policymakers are caught in a difficult position. They must choose between enhanced surveillance and upholding American civil liberties. As the U.S. government continues to determine where to draw the line between national security and civil liberties, it is important to consider the ethical challenges associated with both sides of the debate.

Reference List

Alsabah, N. (2017, March 18). China's quest for cybersecurity causes headache for foreign companies. *The Diplomat*. Retrieved from https://thediplomat.com/2017/03/chinas-quest-for-cybersecurity-causes-headache-for-foreign-companies/

Apple Inc. (n.d.). Our approach to privacy. Retrieved December 3, 2017, from https://www.apple.com/privacy/approach-to-privacy/

Baker, P. (2015, June 1). In debate over Patriot Act, lawmakers weigh risks vs. liberty. *New York Times*. Retrieved from https://www.nytimes.com/2015/06/02/us/politics/in-debate-over-patriot-act-lawmakers-weigh-risks-vs-liberty.html

Brown, P., & Perez, E. (2014, October 12). FBI tells Apple, Google their privacy efforts could hamstring investigations. *CNN*. Retrieved from http://www.cnn.com/2014/09/25/politics/fbi-apple-google-privacy/index.html

Doyle, C. (2012). *Privacy: An overview of the Electronic Communications Privacy Act* (CRS Report No. R1733). Congressional Research Service. Retrieved from https://www.hsdl.org/?view&did=725508

Edward Snowden: Leaks that exposed US spy programme. (2014, January 17). *BBC*. Retrieved from http://www.bbc.com/news/world-us-canada-23123964

Electronic Communications Privacy Act (ECPA). (n.d.). *Electronic Privacy Information Center.* Retrieved from https://epic.org/privacy/ecpa/

Director discusses encryption, Patriot Act provisions. (2005, May 20). *FBI: News*. Retrieved from https://www.fbi.gov/news/stories/director-discusses-encryption-patriot-act-provisions

Figliola, P. M. (2007). *Digital surveillance: The Communications Assistance for Law Enforcement Act* (CRS Report No. RL30677). Congressional Research Service. Retrieved from https://stanford.edu/~jmayer/law696/week8/CRS%20on%20CALEA.pdf

Finklea, K. (2016). *Encryption and evolving technology: Implications for U.S. law enforcement investigations* (CRS Report No. R44187). Congressional Research Service. Retrieved from https://fas.org/sgp/crs/misc/R44187.pdf

Going dark. (n.d.). *FBI*. Retrieved from https://www.fbi.gov/services/operational-technology/going-dark

Gross, G. (2015, April 30). Lawmakers criticize FBI's request for encryption back doors. *InfoWorld*. Retrieved from https://www.infoworld.com/article/2916526/government/lawmakers-criticize-fbis-request-for-encryption-back-doors.html

Homeland Security Committee. (2016). *Going dark, going forward: A primer on the encryption debate* [Majority staff report]. Retrieved from https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf

Kopel, D. B. (1998). When you call, who is listening? *Cato Institute*. Retrieved from https://www.cato.org/publications/commentary/when-you-call-who-is-listening

Kravets, D. (2012, November 2). Feds ordered to disclose data about wiretap backdoors. *Wired*. Retrieved from https://www.wired.com/2012/11/fbi-wiretap-backdoors/

Mason, J. (2015, March 2). Exclusive: Obama sharply criticizes China's plans for new technology rules. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-obama-china/exclusive-obama-sharply-criticizes-chinas-plans-for-new-technology-rules-idUSKBN0LY2H520150302

Olsen, M., Schneier, B., & Zittrain, J. (2016). *Don't panic: Making progress on the "going dark" debate*. Berkman Center for Internet & Society at Harvard University. Retrieved from https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Pierson, D. (2016, February 19). Why Apple's fight with the FBI could have reverberations in China. *Los Angeles Times*. Retrieved from http://www.latimes.com/business/technology/la-fi-tn-apple-global-privacy-20160219-story.html

Popper, B. (2017, May 17). Google announces over 2 billion monthly active devices on Android. *The Verge*. Retrieved from https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users

Price, R. (2016, February 17). Why the FBI is demanding that Apple hack into an

iPhone — and why Apple says it's a terrible idea. *Business Insider*. Retrieved from http://www.businessinsider.com/apple-challenges-fbi-demand-to-hack-into-san-bernadino-shooter-iphone-5c-court-order-2016-2

Savage, C. (2011, February 17). As online communications stymie wiretaps, lawmakers debate solutions. *New York Times*. Retrieved from http://www.nytimes.com/2011/02/18/us/18wiretap.html

Segal, A., & Grigsby, A. (2016, March 15). 3 realistic solutions to prevent another FBI-Apple fight over encryption. *Los Angeles Times*. Retrieved from http://www.latimes.com/business/technology/la-fi-0315-the-download-encryption-20160315-story.html

Statt, N. (2016, January 26). 1 billion Apple devices are in active use around the world. *The Verg*e. Retrieved from https://www.theverge.com/2016/1/26/10835748/apple-devices-active-1-billion-iphone-ipad-io

Sunset Provisions of the USA Patriot Act: Hearing before the Senate Committee on the Judiciary (testimony of Robert Mueller), 109th Cong. (2005). Retrieved from https://archives.fbi.gov/archives/news/testimony/sunset-provisions-of-the-usa-patriot-act-1

Thomas, P. (2015, December 9). Feds challenged by encrypted devices of San Bernardino attackers. *ABC News*. Retrieved from http://abcnews.go.com/US/feds-challenged-encrypted-devices-san-bernardino-attackers/story?id=35680875

Timm, T. (2015, June 9). If the FBI has a backdoor to Facebook or Apple encryption, we are less safe. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2015/jun/09/fbi-facebook-backdoor-apple-encryption-less-safe-privacy

Udry, S. (2015, November 23). The FBI's "going dark" problem: What you need to know. *Defending Rights & Dissent*. Retrieved from https://rightsanddissent.org/news/the-fbis-going-dark-problem-what-you-need-to-know/

U.S. Department of Justice. (2013a). *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22*. Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

U.S. Department of Justice. (2013b). *Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*. Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284

Volz, D., Mimms, S., & Fox, L. (2015, June 2). Senate passes major NSA reform bill. *The Atlantic*. Retrieved from https://www.theatlantic.com/politics/archive/2015/06/senate-passes-major-nsa-reform-bill/445959/

Yadron, D. (2016, March 15). Apple tells judge that US government is well-meaning but wrong in privacy fight. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/mar/15/apple-v-fbi-encryption-privacy-fight-legal-filing