Spring 5-20-2019

"Going Dark" – The Challenge Facing Law Enforcement in the 21st Century

James Christie
La Salle University, christiej3@student.lasalle.edu

“Going Dark” – The Challenge Facing Law Enforcement in the 21st Century

James E. Christie Jr.

LaSalle University

Table of Contents

Introduction

Understanding the "Going Dark" Problem

The role of law enforcement on all levels is to prevent, detect, and investigate criminal activity. A fundamental function of law enforcement is to collect intelligence and evidence to combat criminal and terrorist activity. In numerous instances, intelligence and evidence of criminal activity appear in the form of communications and electronic data. To be effective, law enforcement requires the ability to intercept and access these communications and the electronic data pursuant to legal authority.

However, due to rapidly advancing and evolving technologies utilizing encryption with communication services and securing electronic data, law enforcement is faced with growing obstacles and challenges collecting and extracting evidence and intelligence from these communication platforms. These obstacles and challenges are enhanced because law enforcement often lacks the technical ability to obtain the evidence due to a fundamental shift in the methods utilized by communication services and technologies. This fundamental shift is a phenomenon in the law enforcement community known as the "Going Dark" problem. "Going Dark" can be defined as "the effect of encryption technology embedded in commercially available cell phones and communications technologies that allow individuals to easily and effectively prevent access to their electronic devices, communications and digitally stored data" (as cited in Corn, 2015, p.1433). More clearly stated by former Federal Bureau of Investigation (FBI) Director James Comey, "Going Dark" is 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" (Comey, 2014).

Critics contend the "Going Dark" issue had been resolved almost twenty years ago. From their perspective any further attempts to address the "Going Dark" issue will weaken information and data security, encroach on the civil liberties of Americans, and place American companies at an economic disadvantage.

The challenges encrypted data and the "Going Dark" problem causes for United States (U.S.) law enforcement will be the focus of this research paper. Specifically addressed will be the history of the debate, obstacles encountered by law enforcement, the arguments on both sides of the fence, constitutional and economic considerations, case examples, and potential solutions. Ultimately, this research paper will confront the question of whether "Going Dark" a legitimate concern which needs to be addressed through a national discussion to develop global solutions or is it an issue over exaggerated, already resolved, and better left alone.

Defining Cryptography and Encryption

Simply defined, cryptography is the science of encryption. The origin of cryptography dates back thousands of years and is believed to be as old as written forms of communication (Kerr & Schneier, 2018). Encryption is defined as a centuries old technique which utilizes mathematical algorithms to transform readable forms of messages and communications to unreadable codes (Kerr & Schneier, 2018). Both the senders and receivers require a key to decrypt the encrypted messages. For instance, users of encrypted communication applications, such as Telegram Messenger, the key is generally created and exchanged between the users' devices without the users ever having to enter the encryption key. The key is automatically generated and exchanged by the encrypted application's software to allow for the encrypted communications between the users (Kerr & Schneier, 2018).

The purpose of encrypting messages and communication is to prevent them from being intercepted and read by unauthorized third parties (Schulze, 2017). An encryption algorithm is a series of operations performed on information that encodes the information to make it unreadable (Kerr & Schneier, 2018). Encryption algorithms can be simple or highly complex depending on the need and their purpose (Kerr & Schneier, 2018). Today's encryption algorithms rely on highly complex mathematical formulas and follow Kerckhoff's Principle. Kerckhoff's Principle was established by Dutch cryptographer Auguste Kerckhoff's in the 1800s and states "an encryption algorithm should be secure if everything is known about it except the key" (as cited in Kerr & Schneier, 2018, p. 993).

As mentioned above, in order to unlock an encryption algorithm a special code, known as the key, is paired with the known algorithm to encrypt or decrypt the data (Kerr & Schneier, 2018). Essentially, a key is a string of data made up of information known as "bits", consisting of zeroes and ones (Kerr & Schneier, 2018). In general, the larger number of bits in a key the stronger the encryption (Kerr & Schneier, 2018). As a reference, the majority of encryption keys currently being utilized are normally 128 or 256 bits long (Kerr & Schneier, 2018). In today's world any type of electronic data or information can be easily and at little cost encrypted with 128-bit or 256-bit keys, such as emails, text messages, videos, photographs, or programs. Currently, it is believed key lengths of 128-bits or more are unable to be defeated by brute force attacks conducted by any of the world's premier intelligence or law enforcement agencies (Kerr & Schneier, 2018).

Understanding Electronic Data "at rest" and "in motion"

The technological advances in the latter part of the 20th Century and throughout the 21st Century were unimaginable fifty years ago. In today's society, the vast majority of Americans

carry personal electronic devices (PEDs) which serve as phones, cameras, global positioning systems (GPS), and computers, all in one device. PEDs are so prevalent in American society that, according to a 2018 Pew Research survey, 77% of Americans now own a smartphone. Each one of these PEDs can store enormous amounts of data and information. Ray Canetti, a cryptography expert and professor at Boston University, commented smartphones now have the same parts and capabilities of personal computers of 15 years ago (House Homeland Security Committee, 2016). Additionally, PEDs can be utilized by their users to communicate over a number of technology-based platforms. In today's world, a significant amount of data and information which is sent, received, and stored on our PEDs is encrypted. This encrypted data can be categorized as either "in motion" or "at rest" and each creating their own distinct challenges for law enforcement.

In order to understand and fully comprehend the "Going Dark" debate, these two intersecting challenges must be clearly defined and discussed. The first challenge is end-to-end encryption which is also known as "data in motion" or "messages in motion". End-to-end encryption more clearly defined is the encryption of messages and communications in motion between a sender and the intended recipient (Manpearl, 2017). With end-to-end encryption, only the sender and recipient possess keys to decrypt the message (Manpearl, 2017). For example, encrypted "messages in motion" could be anything from phone calls and text messages to emails and real-time instant messaging (Manpearl, 2017).

Traditionally, law enforcement would monitor and capture "messages in motion" through court authorized wiretaps. In 1994, with the passage of the Communications Assistance to Law Enforcement Act (CALEA), telecommunication carriers were required to ensure their networks could be electronically surveilled or more commonly known as "wiretapped" pursuant to a court

order (Manpearl, 2018). This act addressed concerns from law enforcement because telecommunication carriers were shifting their technologies from copper wires to fiber optics which made traditional wiretapping techniques obsolete (Manpearl, 2017). CALEA was important because it allowed law enforcement to conduct electronic surveillance on new technologies at the time, such as wireless services (Manpearl, 2017). However, CALEA failed to address the issue of encryption and even included verbiage indicating telecommunication carriers were not responsible for decrypting communications independently encrypted by the subscriber or customer (Manpearl, 2017). A second concern for present day law enforcement is CALEA does not address today's Internet based communication services which offer encryption as part of their business models. These Internet based communication services are primary examples of "messages in motion" such as email, instant messaging, social media sites, or peer-to-peer services (Manpearl, 2017).

The second challenge is encrypted data and information stored on a device called endpoint encryption, also known as "data at rest" (Manpearl, 2017). For example, endpoint encryption could be anything you store on your cellular telephone such as emails, text messages, calendars, contacts, photos, and videos. The majority of the popular PEDs owned by Americans are produced by technology giants such as Apple and Google which offer the option of encrypting the data stored on their device. Additionally, as discussed further in this research paper, the current trend is for technology companies to enable encryption as the default setting in their devices instead of the opposite.

Origins of the "Going Dark" Problem: Crypto Wars

Crypto Wars 1.0

The debate regarding encryption has been raging for decades. The origins of the "Crypto Wars" began in the 1970's, when the National Security Agency (NSA) and other agencies within the United States Intelligence Community (USIC) supported placing restrictions on technology companies and cryptographic research (Manpearl, 2017). These restrictions occurred in two forms. First, technology companies were restricted from exporting encryption technology to foreign countries (Manpearl, 2017). Second, prohibitions were placed on researchers from publishing their cryptographic research and advances (Manpearl, 2017).

The "Crypto Wars" intensified in the 1990s as encryption became more prevalent and technology companies became more invested in encryption technologies (Manpearl, 2017). This issue was exacerbated by the explosion onto the market of relatively affordable computers with enough processing power to encrypt data and information which made it difficult, if not impossible, for law enforcement and the USIC to decipher (Manpearl, 2017). Based on these factors, federal law enforcement agencies, particularly the FBI, feared the spread of encryption would adversely impact national security and criminal investigations. Subsequently, federal law enforcement joined the debate and partnered with the USIC to limit the advancement of encryption technologies (Manpearl, 2017).

At the same time, opponents on the other side of the debate, such as technology companies, technology researchers, and civil libertarians vehemently opposed the government's efforts to limit encryption and technology surrounding it. Technology companies and technology researchers argued the development and use of encryption was necessary, as the Internet developed along with the trend to store information electronically increased

exponentially. Many experts on the encryption side of the debate believed strong encryption was required to strengthen information security and protect the nation's critical infrastructure and financial institutions. The civil libertarians argued the need for increased privacy for companies and citizens and that the export restrictions enacted by the government violated cryptographers First Amendment rights of free speech (Manpearl, 2017).

Throughout the 1990s, the U.S. government continued their efforts to restrict the export of encryption technology and limit its use (Manpearl, 2017). One suggested solution to the government's issue with the private use of encryption technology was the proposal to use an encryption key which would be held by the government or a neutral third party (Manpearl, 2017). The key could then be accessed by the government for lawful purposes to unlock the encryption. Based on the premise of developing an encryption key and holding it in escrow, the NSA developed a key escrow system known as the Clipper Chip (Manpearl, 2017). The NSA developed the Clipper Chip with an encryption key for use with telephones to allow for encrypted and secure communications (Manpearl, 2017). Use of the Clipper Chip by private companies and entities was voluntarily, but to encourage its use throughout the country, the government made it the federal standard (Manpearl, 2017). The USIC and law enforcement agencies were hopeful this would encourage its use because entities which engaged in business with the federal government would need to implement this federal standard (Manpearl, 2017). The idea and use of the Clipper Chip were quickly confronted by computer experts, technology companies, and privacy advocates who felt the government was inhibiting business and violating their privacy rights (Manpearl, 2017). Additionally, soon after the Clipper Chip was introduced to consumers in early 1993, Matt Blaze, a cryptographer identified vulnerabilities within the Clipper Chip technology. This discovery ultimately led to the demise of the Clipper Chip and its

use in the private sector (Manpearl, 2017). It was estimated by the National Research Council only 10,000 to 15,000 Clipper Chip enabled phones were ever sold and mostly to the government and its contractors (Schulze, 2017). The failure of the Clipper Chip is considered by many observers of this debate as the turning point of Crypto Wars 1.0 and the subsequent defeat of the U.S. Government's efforts to limit encryption. According to General Michael Hayden former NSA Director, the NSA and the U.S. Government lost Crypto War 1.0: "We didn't get the Clipper Chip, we didn't get the back door" (as cited in Schulze, 2017, p.55).

In 1994 the U.S. Government relaxed its strict opposition to the development and use of encryption in the private sectors, as evident in the passing of the Communications Assistance to Law Enforcement Act (CALEA). The passing of CALEA required telecommunication carriers to alter and modify their equipment and services in order to ensure they had the ability to comply with legally authorized orders of electronic surveillance. This allowed law enforcement to continue to conduct electronic surveillance, despite the institution of new and emerging digital technologies and wireless services offered by the telecommunications industry (Manpearl, 2017). However, CALEA failed to address the issue of encryption for law enforcement. In fact, CALEA included language indicating a telecommunications carrier was not responsible for decrypting or ensuring the government could not force a company to build a backdoor to their encrypted technology (Manpearl, 2017). It is also important to note, CALEA was written with a focus on telecommunication carriers, not Internet-based communications companies which currently dominate the market place. This is an important distinction because it can be argued CALEA is outdated since it does not address any of the current day Internet-based communications, such as email, instant messaging, social media sites, or peer to peer services and applications (Manpearl, 2017).

A second way the government tried to control and prevent the spread of encryption technology in the 1990s was by placing it on the U.S. Munitions List which strictly limited its sale and exportation (Manpearl, 2017). By being placed on the U.S. Munitions List, encryption technology was considered a defense technology and oversight of its foreign sales were heavily monitored by the Department of State (Manpearl, 2017). In 1996, after much debate, President Clinton removed commercial encryption from the U.S. Munitions List (Manpearl, 2017). However, this only allowed technology businesses to sell an "export grade" encryption to overseas vendors. This "export grade" encryption was a significant downgrade from the far superior encryption on the market at that time (Manpearl, 2017). Subsequently, a federal lawsuit was filed and in 1999 the U.S. Ninth Circuit Court of Appeals ruled the government controls on encryption technology violated cryptographers' First Amendment rights to free speech because it prohibited them from publishing their source code (Manpearl, 2017).

Ultimately, the government conceded its efforts to limit the use and spread of encryption technology. A general consensus was reached by government and private sector experts that the advantages of encryption and cryptography outweighed the disadvantages (Schulze, 2017). This was confirmed in September 1999 when the Clinton Administration updated their policies regarding encryption and virtually relaxed all of their restrictions on exporting encryption technologies (Schulze, 2017).

Crypto Wars 2.0

The emergence of a second round of "Crypto Wars," dubbed Crypto Wars 2.0, came about approximately ten years later, sparked mainly by concerns of growing instances of "Going Dark" by the FBI (Manpearl, 2017). The concerns stemmed from the FBI increasingly lacking the ability to access encrypted data, information, and electronic communications during the

course of investigations in which they had the legally authority to access or intercept it. As the use of encryption became more prevalent, the "Going Dark" problem became more pronounced and began to significantly impede the criminal investigations of federal, state, and local law enforcement agencies around the country. The "Going Dark" issue is even more magnified on the state and local levels because of their limited amount of investigative resources and technical capabilities, as compared to federal law enforcement agencies (Manpearl, 2017). Additionally, U.S. intelligence agencies, such as the Central Intelligence Agency (CIA) and NSA, faced similar challenges with their intelligence collection capabilities due to the increased use of encryption by our foreign adversaries. However, the USIC has greater resources and much less legal restraints to combat the challenges from encryption than U.S. law enforcement agencies (Manpearl, 2017).

The "Going Dark" debate re-emerged from the 1990s for two primary reasons. First, technology companies, such as Apple and Google, began to increasingly enable encryption as the default setting on their electronic devices (Manpearl, 2017). In essence, all the data and information stored on Apple's electronic devices, for instance iPhones, iPads, and MacBook computers, was automatically encrypted. This information remains encrypted unless the owner of the device makes a concerted effort to disable the encryption capability on their device. For example, in 2014 Apple announced all of its devices utilizing their iOS 8 mobile operating system would have the setting of default encryption (Manpearl, 2017). Subsequently, Google followed Apple's lead enabling encryption as the default setting on its Android operating system (Manpearl, 2017). This simple modification was significant because the use of encryption is favored, unless the device's owner takes specific action to disable it. A second factor was that internet service providers began to offer a wide range of services and products encrypting data

both "at rest" and "in motion". These types of services included but were not limited to encrypted cloud storage systems and communication platforms which utilize end-to-end encryption (Manpearl, 2017). Most technology companies, such as Google, Apple, and Microsoft, offer encrypted cloud storage and computing services. They also offer popular end-to-end encryption communication platforms in today's market to include iMessage, Whatsapp, Telegram, and Wickr. The critical point is the technology companies which offer these products and services were not required by CALEA and did not build into their storage, communication platforms, and systems the technical capabilities to decrypt their customers' data "at rest" and "in motion". These companies, even if they were instructed to do so via a lawful court order, most likely do not have the ability to decrypt their customers data (Manpearl, 2017).

As a result of this mounting "Going Dark" problem, law enforcement and intelligence officials began to sound the alarm regarding the challenges they faced from the increased use of encryption. Their main concern was that the use of encryption by terrorists and criminals would prevent them from disrupting the next terrorist attack, prevent them from locating a kidnapping victim, or convicting a child predator (Manpearl, 2017).

At the time, FBI Director James Comey became the most vocal voice raising the "Going Dark" problem facing law enforcement. In October 2014, Director Comey gave a speech at the Brookings Institution raising awareness on the "Going Dark" problem from the law enforcement perspective. In his speech, Director Comey (2014) indicated he wanted to begin a national dialogue on how emerging technologies impacted law enforcement and overall public safety. Director Comey (2014) raised the concern current U.S. laws have failed to keep pace with technology. He noted, many times law enforcement has the legal predication and authority to access data and communications, but lack the technical capabilities to do it. Director Comey

(2014) highlighted law enforcement's major concern with the "Going Dark" problem, which was in one facet, they were losing their ability to collect critical evidence of child predators, violent criminals, or a terrorist cell planning or conducting an attack, because they were utilizing encrypted communication devices and platforms. During the speech, Director Comey (2014) confronted head on the misperception that law enforcement was advocating for technology companies to build a "back door" into their technology devices and systems which could be exploited by hackers and rogue nation states. Director Comey (2014) promoted an approach of dialogue between technology companies, privacy advocates, law enforcement, and legislators, in which a discussion could be begin to occur. Director Comey (2014) was hopeful these types of discussions could lead to clear policy and legislation being created to enable law enforcement to enter the front door in a transparent manner to collect the evidence they are legal authorized to access. By allowing "front door" access, this would enable technology companies and program developers to incorporate access capabilities and intercept solutions for law enforcement. It would also allow them to consider security risks and develop security features in the forefront during the design phase, instead of after the fact with patchwork solutions.

"Going Dark" Debate: Arguments for a Lawful Access Requirement

It is common knowledge the primary role of the U.S. Government is to protect and defend the safety and security of its citizens and nation as a whole. This concept was reinforced in the U.S. Supreme Court's proclamation in Haig v. Agee that "no governmental interest is more compelling than the security of the Nation" (as cited in Dunlap, 2017, p.1688). With the development of a global economy and the birth of 21st Century technology, a wide range of threats and challenges have emerged, unimaginable to our nation's founding fathers. One of those emerging threats is the increased use of encryption technology by criminals and terrorist

organizations to plan and conceal their criminal activities from law enforcement. For this reason, the "Going Dark" issue is a great concern for law enforcement and the USIC.

"Going Dark" - A Threat to Public Safety and to National Security

The previously referenced Pew Research study determined 95% of Americans own cell phones and 77% of Americans own smartphones. In addition, nearly three quarters of Americans own a desktop or laptop computer. As discussed, these devices are being utilized in every aspect on an individual's life such as communicating, web browsing, social media, travelling, and storage of sensitive information and records. The use of PEDs are interwoven within our daily lives and in many ways are a necessity. As expected, PED users are more adept at and inclined to utilize encryption as a security feature to safeguard their activities and information (House Homeland Security Committee, 2016). Similarly, criminals and terrorists are more prone to use these technologies, such as end-to-end and endpoint encryption, to covertly conduct their criminal and terrorist activities. As the use of encryption expands, by both the victims of crime and the perpetrators themselves, a plethora of evidence and intelligence has been and will continue to be locked away from investigators and prosecutors (Manpearl, 2017). For instance, over a nineteen-month period between 2014 thru 2016, the Office of the District Attorney for New York County documented more than 175 criminal investigations in which they incurred obstacles accessing digital evidence (House Homeland Security Committee, 2016). In Los Angeles in 2016, criminal investigators were unable to access over 300 PEDs safeguarded with encryption (Manpearl 2017). Furthermore, Director Comey indicated between October 2016 and December 2016, the FBI did not possess the technical capabilities to access 1,200 out of 2,800 PEDs which were sent to them for access and evidentiary purposes by law enforcement agencies at all levels (Manpearl 2017). These statistics represent a mere fraction of the

encrypted PEDs locked containing critical evidence and intelligence inaccessible to law enforcement on a national level.

It should also be noted regarding data stored on an individual's PED protected by endpoint encryption, federal appeals courts have ruled the Fifth Amendment, under the Self-Incrimination clause, prohibits the courts and law enforcement from compelling the owner/user of a PED to divulge their password (Potapchuk, 2016). This is obviously significant because it reduces the options law enforcement have to legally access data on an encrypted device. It is logical to assume in most cases, only the owner/user knows their password to access the device, further limiting investigators' options to access the information.

It is extremely difficult to quantify the challenge created for law enforcement in trying to monitor the active communications of criminals and terrorists using end-to-end encryption. The reason being law enforcement does not waste the time and resources to apply for court orders to electronically surveil communication platforms which they know employ end-to-end encryption by default (Manpearl, 2017). Law enforcement views this lack of surveillance capability as an enormous blind spot and vulnerability. And criminals and terrorists are aware of this vulnerability and are exploiting it. This point was reiterated by FBI Director Comey in a 2015 statement before the Senate Select Committee on Intelligence. FBI Director Comey (2015) testified that ISIS operators in Syria are "recruiting and tasking dozens of troubled Americans to kill people [using] a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment" (as cited in Zittrain, Olsen, O'Brien, & Schneier, 2016, p.7). Additionally, in 2015 Director Comey remarked at a Senate Judiciary Committee, the FBI has experienced, through counterterrorism investigations, scenarios in which ISIS operatives begin

conversing with newcomers and then direct them to switch to an end-to-end encrypted mobile messaging application (Bennett, 2015). Once this occurred, the FBI lost visibility into those future communications (Bennett, 2015). This strategy indicates encrypted mobile messaging applications have become part of a terrorist's tool box to avoid electronic surveillance of law enforcement (Bennett, 2015).

Based on the aforementioned statistics and factors, it is evident the "Going Dark" issue will continue to be a significant obstacle for law enforcement. This challenge has direct implications on national security and public safety. The primary reason being is bad actors will continue to subvert law enforcement's efforts by concealing their communications, plans, and nefarious activities by utilizing encryption as a tool. By not developing a solution to the "Going Dark" problem, it will continue to adversely impact law enforcement's abilities with preventing and solving crimes of violence, such as murders, sexual assaults, and robberies, and acts of terrorism. It is no secret our countries' enemies are continually plotting ways to conduct devastating terrorist attacks on our nation and against our citizens. What is troubling is the "Going Dark" threat could potentially prevent law enforcement from uncovering a plot and preventing a devastating terrorist attack against our nation's citizens or critical infrastructure on the scale of the 9/11 attacks. This statement should not be considered fear mongering it is simply a present-day reality.

Fourth Amendment Supports a Lawful Access Requirement

As previously discussed, a nation must make the protection of its citizens a primary objective. However, the measures the government, including law enforcement, can employ to provide these protections must remain within the boundaries of the U.S. Constitution. More

specifically, concerning the "Going Dark" issue, its actions must be acceptable under the Fourth Amendment. The Fourth Amendment of the U.S. Constitution states,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Const. amend. IV).

As it relates to the "Going Dark" debate, the Fourth Amendment provides no restrictions which would preclude Congress from passing laws allowing the government to have reasonable access to encrypted data (Corn, 2017). Operating under this legal standard, Congress could enact legislation requiring companies which offer encrypted communication services not covered by CALEA to provide lawful intercept capabilities to law enforcement.

Further analysis indicates the Fourth Amendment permits legal searches and surveillance when deemed reasonable (Corn, 2015). The concept of "reasonableness" is central to any challenges to the Fourth Amendment (Corn, 2017). Corn argued reasonableness is consistently defined by "balancing individual privacy with societal interests in effective law enforcement" (as cited in Corn, 2017, p. 346). The interpretation of the Fourth Amendment does not provide citizens and the technology companies with an absolute right to an inaccessible "dark area" to law enforcement (Corn, 2017). It only provides an absolute right to be secure against unreasonable searches and seizures of persons, homes, papers, and effects. Under this constitutional premise, legislation could also be passed by Congress requiring technology companies to equip their encrypted products and devices with the ability to be accessed when legally authorized pursuant to a search warrant or court order. The key aspect to any type of

legislation intended to address the "Going Dark" issue will be to strike a reasonable balance between government intrusion (security) and citizen's privacy (Corn, 2017).

A potential constitutional argument would be focused on legislation which granted a lawful access requirement mandating technology companies to assist law enforcement armed with a court order. This type of law would require technology companies to develop and disclose a key to access the data within their encryption technologies. Such a law could be potentially challenged as being in violation of the Fourth Amendment, which provides citizens with the right to be secure in their "papers and effects". Based on the aforementioned legal analysis and prior rulings, this type of challenge would most likely fail.

Congress has been studying these issues for several years, but has failed to act. The fact remains, due to evolving encryption technologies law enforcement has been denied access to communications and electronic data in circumstances which fall within the legal parameters of the Fourth Amendment and statutory standards. Ultimately, law enforcement is not pursuing avenues to expand their authorities to access data or conduct legal surveillance to monitor communications (Comey, 2014). Law enforcement is simply seeking solutions to keep pace with technology in order to maintain their sworn obligation to protect the citizens of the United States.

"Going Dark" Debate: Arguments Against a Lawful Access Requirement

As a result of the "Going Dark" phenomenon, the debate of liberty versus security, which can be traced back to the founding fathers of our nation, has intensified. Advocates of liberty and privacy frequently point to Benjamin Franklin's famous quote of: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." (as cited Alhogbani, 2015, p. 484). This premise is flawed because law enforcement is not seeking

to restrict an "essential liberty" which is further explained below. Privacy advocates focus their arguments around three points. To begin, they fear government efforts to force technology companies to build in vulnerabilities within their encryption technologies compromises the privacy and security for all encryption users (Schulze, 2017). Next, the economic implications to U.S. technology companies and the government's interference in a free market are challenged (Schulze, 2017). Finally, there are civil liberty concerns for depredation of citizens privacy rights and the expansion of governmental control over its citizens (Schulze, 2017). Each of these three concerns will be specifically addressed below.

Security Concerns and Vulnerabilities

In order to delve into the core of this debate, a starting point is to understand the concerns and arguments for privacy and security advocates in their desire for strong and secure encryption. In today's digital age, encryption is utilized throughout the world as a security feature to secure sensitive and personal information. For instance, encryption is utilized by all levels of the U.S. Government to safeguard critical infrastructure, classified and sensitive information, and the communications of military and government officials (Manpearl, 2017). Additionally, encryption is employed by the private sector to secure banking and financial transactions, trade secrets, and personal communications and information. The major concern is that if technology companies built third party access into their encryption software for law enforcement use through technological architecture or also referred to as a "back door," this would create security vulnerabilities which could be and have been exploited by talented hackers and adversarial nation states (Manpearl, 2017). This is a legitimate concern as highlighted by the security flaws of the aforementioned Clipper Chip. Individuals' privacy and security could be jeopardized to a certain extent if a "back door" for lawful access was required by law. An extra concern is if this type of legal requirement became a reality, it would also pose an added

vulnerability to the U.S. Government's critical infrastructure and sensitive information which relies heavily on encryption as a cyber-security measure (Manpearl, 2017).

However, the strongest counter argument to the security fears regarding the lawful access requirement, is law enforcement and intelligence agencies are fully vested with ensuring a secure solution is obtained. They understand the nation's critical infrastructure and their agencies' information and operations could be attacked and compromised if a solution with weak security and vulnerabilities was moved forward. More importantly, law enforcement is not asking for access through an unsecured backdoor. Law enforcement is requesting for the digital equivalent of a secured fortified "front door" with locks and bars (Corn, 2015). It is well within reason to believe technology industry security experts and cryptographers can develop a secure "front door" for lawful access. And with the development of a secure "front door" to provide lawful access, security experts can plan to constantly prod it for vulnerabilities and weaknesses. In fact, this is currently being done to a certain extent by Google and Apple (Manpearl, 2017). In order to target its customers for advertisements, Google has the capabilities to decrypt Gmail and Gchat communications (Manpearl, 2017). Apple employs software that allows its iCloud backups to occur in a way they can be decrypted (Manpearl, 2017). Ultimately, by creating solutions for lawful access during the design and development phase of encryption, technology will be much more secure than to exploit vulnerabilities after the fact (Comey, 2014). This type of cooperation between the government and the private sector will increase overall security while reducing vulnerabilities and "back door" breaches (Corn, 2017)

A second security trepidation is any type of lawful access requirement would require an encryption key be developed and stored by either the technology companies, government, or a third-party entity (Manpearl, 2017). The holders of the encryption key would quickly become

targets of hackers and adversarial nation states (Manpearl, 2017). Additionally, countries with less or no legal standards could require technology companies, such as Apple, whose products are marketed globally, to provide their government with a copy of the encrypted key in order for Apple to continue doing business in their economies.

Security procedures are currently in place to continuously safeguard high level and Top-Secret information by both private sector entities and governmental agencies. Similar protocols would be enacted to successfully secure an encryption key which can provide lawful access as needed. One such protocol could be to split the key and secure it in separate places. As an added measure, in theory developers of the encryption key could equip it with a self-destruction feature or have the ability to remotely wipe it, in the event it ever became compromised. In regards, to foreign countries requiring access to a technology company's encryption key, this could create complexities and challenges. Numerous foreign countries have lower legal standards as compared to the U.S. and could seek access to the encryption key with little or no legal justification. However, this could be addressed through international laws and treaties focusing on encryption which can set legal precedent and standards with participating countries to help protect the technology companies.

A final security consideration is providing lawful access does not eliminate the fact that there are numerous encrypted technologies produced outside the U.S. which are commercially accessible to criminals and terrorists (Manpearl, 2017). Sophisticated criminals and terrorists would be able to encrypt their illicit conversations and information utilizing these services (Manpearl, 2017). This is a reality, but the majority of criminals and terrorists are not sophisticated (Manpearl, 2017). Additionally, U.S. companies currently lead and control the market with products utilizing encryption technology (Manpearl, 2017). Another significant

leverage point is the majority of the worldwide Internet and wireless communications transit through U.S. infrastructure (Manpearl, 2017). This reality could force foreign technology companies to comply with U.S. legislation addressing "Going Dark" concerns or face losing access which would greatly reduce their reliability and coverage areas. Another area to consider, is by requiring lawful access, it would considerably narrow the capabilities and options for bad actors, while lawfully increasing the percentages for law enforcement and the USIC to identify illicit activity and threats to national security.

Economic Considerations

Today's global economy is fueled by and relies on the ease of digital communications. It is imperative these communications remain secure. Encryption is widely used by numerous industries to secure their communications, information, and customers' data. For example, it is estimated 44% of the global encryption software market is attributed to the financial industry (House Homeland Security Committee, 2016). Another aspect is e-commerce and online retail sales which rely heavily on encryption to secure their transactions and customers' data. E-commerce is a substantial and growing component to the U.S. economy. In 2015, the U.S. Department of Commerce estimated e-commerce sales at $314.7 billion (House Homeland Security Committee, 2016). If legislation was passed in the U.S. granting lawful access, it could potentially have a devasting impact on U.S. based companies' ability to compete globally. Consumers may look to foreign technology companies and products due to security fears. An additional complexity in this dynamic is the Edward Snowden leaks of U.S. intelligence's abilities and activities in 2013 (Manpearl, 2017). Snowden's leaks have raised the anxiety levels of citizens both foreign and domestic about the surveillance capabilities of the USIC. If lawful access legislation was enacted, American and foreign consumers may be more reluctant to use

American companies' technologies if they believed they could be comprised and accessed by U.S. law enforcement and the USIC (Manpearl, 2017). This potential reduction of U.S. technology companies in the market share would impact their profitability and economic competitiveness (Manpearl, 2017). For instance, over a three-year period after the Snowden revelations, U.S. technology companies attributed loss amounts to the scandal somewhere between $35 and $180 billion in sales (Manpearl, 2017). However, based on history, these economic concerns may be overstated. The counter argument is consumers' privacy concerns are heavily outweighed by their desires for convenience, reliability, and the capabilities of their devices. Consumers generally appear to be willing to sacrifice security and privacy to possess the cutting edge in technology (Manpearl, 2017). If the past is a predicter of the future, U.S. technology companies will continue to dominate the technology sector market even if lawful access legislation is passed (Manpearl, 2017). The driving factor for this belief is U.S. technology companies' ingenuity and adaptability will continue to produce the most desirable and technologically advanced devices and services.

Civil Liberty and Privacy Concerns

From the inception of the Crypto Wars in the 1970s, the focal point of the encryption debate has been privacy vs. national security. Civil liberty activists fear any type of government proposed solution to the "Going Dark" issue would diminish privacy and expand governmental powers and authorities and be an encroachment on citizens' privacy rights (Schulze, 2017). Encryption is viewed by many as a privacy enhancing technology and further government involvement limiting its use is disconcerting to them. However, the counter argument is, as previously stated, law enforcement is not seeking to expand their surveillance capabilities, they are only seeking solutions to keep pace with technology within their current scope of authority.

Privacy would not be diminished and law enforcement would only be able to surveil communications or access data upon obtaining the properly predicated legal authorization from a duly sworn judge. It is logical to surmise this argument is rooted in privacy advocates contempt for lawful government surveillance.

In the event the U.S. Congress engaged in legislation to limit the use of encryption or requiring technology companies to build access points into their encryption technologies, it can be expected the legislation would be challenged on multiple constitutional issues. The Constitution provides several protections for freedom of speech and privacy which civil liberty advocates may evoke. One probable argument against government restrictions on encryption would center on the logic they violate cryptographers First Amendment right of freedom of speech. Civil liberaltarians could argue encrypted software is a form of speech which is constitutionally protected (Manpearl, 2017). Any type of legal challenge relating to First Amendment issues would not be applicable because law enforcement is not seeking to limit strong encryption, but just the opposite, they are eager to promote secure encryption. Once again, law enforcement only pursues lawful access when deemed reasonable by the courts.

Additionally, since the explosion of the Internet and PEDs, privacy advocates believe the digital environment in which we currently reside, allows for enhanced surveillance by law enforcement and intelligence agencies. Through the increased use of the Internet and PEDs, the amount of information collected and stored concerning consumers' personal habits and location data is enormous and ever growing. Additionally, new opportunities are continually developing for the government to conduct surveillance and data collection with the ever-increasing interconnected network of electronic gadgets, commonly referred to as the Internet of Things (IoT). The IoT permeates present day society with electronic items such as smart televisions,

refrigerators, home security systems, watches, and cars (Zittrain, Olsen, O'Brien, & Schneier, 2016). Most times this information is accessible by law enforcement armed with the appropriate legal process. Some argue access to this additional information diminishes law enforcement's need to surveil encrypted communications of targets of investigations (Zittrain et al., 2016). However, while the opportunities for surveillance may be increasing, through IoT, it does necessarily translate into quality surveillance opportunities which will produce the valuable type of evidence and intelligence sought through communication platforms and devices. Bad actors utilize their PEDs in the same manner as most honest citizens. They frequently carry them on their person, communicate with coconspirators, take photographs of potential targets and victims, and store incriminating digital notes and plans. What is the alternative for law enforcement? Attempt to conduct audio surveillance through a television or refrigerator? It is just not a feasible or practical option to think it would produce the quality of evidence and intelligence able to be obtained from a PED.

It should also be noted, even as the FBI and several agencies within the USIC advocate for solutions to the "Going Dark" issue, there are multiple agencies within the U.S. Government which have a differing point of view. For example, the Defense Advanced Research Projects Agency (DARAPA) supported by the Naval Research Laboratory and the Department of State developed the Tor network which conceals the transactional information of Internet-based communications (Harvard University Berkman Center for Internet & Society, 2016). Simply stated, the TOR network is utilized to provide anonymity by obscuring the Internet Protocol (IP) addresses of the sender and receivers of electronic communications, such as emails, over the Internet. These U.S. Government agencies support the development of strong encryption and the use of TOR for security reasons as well as human-rights matters (Harvard University Berkman

Center for Internet & Society, 2016). TOR and other encrypted communication platforms are widely used by critics of oppressive governments to voice their opposition and conceal their identity. Law enforcement understands and supports the use of TOR and encryption for these endeavors. Any legislative solution passed in the U.S. should not impact TOR or provide an oppressive regime with access to an encryption key.

Critics also argue law enforcement can utilize additional investigative techniques to collect the evidence and intelligence they seek instead of creating added vulnerabilities with encryption technology. Additionally, critics disagree with the impact proposed "Going Dark" solutions would have with mitigating the advantages criminals and terrorists gain from utilizing encryption platforms to communicate and store data (Harvard University Berkman Center for Internet & Society, 2016). Law enforcement professionals strongly disagree with these arguments and believe the most valuable evidence and intelligence can be gleamed from PEDs. This is why the law enforcement officials at all levels have actively reengaged with this debate.

Real World Case Studies Highlighting the Need for Solutions

Data "At Rest" - San Bernardino & Brian Horn Case Studies

On December 2, 2015, Syed Rizwan Farook (hereafter Farook) and Tashfeen Malik (hereafter Malik), a married couple of Pakistani descent, conducted a terrorist attack targeting a San Bernardino County Department of Public Health (SBCDPH) training seminar and Christmas Party at a rented offsite facility (Schmidt & Perez-Pena, 2015). The event was attended by approximately 80 SBCDPH employees (Schmidt & Perez-Pena, 2015). Farook, an employee of the SBCDPH, and his wife employed semi-automatic pistols and rifles to carry out the attack resulting in the murder of fourteen victims and the wounding of twenty-two others (Schmidt & Perez-Pena, 2015). Prior to fleeing the scene, Farook and Malik left behind three improvised

explosive devices (IED) believed to target and injure first responders (Schmidt & Perez-Pena, 2015). Fortunately, due to poor construction the IEDs failed to detonate. Approximately four hours later, law enforcement located Farook and Malik and a vehicle pursuit ensued (Schmidt & Perez-Pena, 2015). After a brief chase, Farook and Malik stopped their vehicle in a residential neighborhood and engaged law enforcement in a fierce gun battle in which two police officers were wounded. Farook and Malik were killed by officers during the firefight (Schmidt & Perez-Pena, 2015).

As a result of the suspected nexus to terrorism, the FBI became the lead investigative agency. An FBI Investigation into the attack classified Farook and Malik as self-radicalized "homegrown violent extremists". Although the investigation failed to determine specifically which foreign terrorist group inspired Farook and Malik, evidence indicated they were self-radicalized through the Internet to conduct jihad (Schmidt & Perez-Pena, 2015).

During the investigation, the FBI recovered Farook's work iPhone which was owned by the SBCDPH. The FBI suspected the phone contained evidence of Farook's criminal and terrorist activities. As the legal owner of Farook's work iPhone, the SBCDPH provided consent to the FBI to search the phone. However, due to Apple's iPhone endpoint encryption security software, the FBI and other government agencies' efforts to access it were thwarted. Next, the FBI requested Apple to voluntarily assist with unlocking the iPhone, but Apple denied their request based on concerns it would degrade the security features on their products. The data "at rest" on the phone was inaccessible due to Apple's endpoint encryption (Dunlap, 2017). Subsequently, the FBI applied for and was granted a federal court order pursuant to the All Writs Act ordering Apple to aid with accessing the phone (Posner, 2016). Apple intended to challenge the court order, but the court order was eventually withdrawn when it was announced the FBI

gained access to the phone (Posner, 2016). The FBI solicited the services of a third party in the private sector to identify a zero-day vulnerability and unlock the phone (Posner, 2016). Ultimately, the phone contained very minimal information deemed relevant for investigators (Posner, 2016).

This case study highlights an excellent example in which law enforcement had a legal authority to access data "at rest" on a PED which was locked due to endpoint encryption. As a result of the FBI being able to gain access to the contents of the device through a third party, the legal arguments suggesting technology companies can be compelled by court orders pursuant to the All Writs Act was never challenged or settled by higher courts. In this case, the contents of the phone were determined to be irrelevant. However, imagine a scenario in which the contents of the phone contained the identities of additional attackers and/or future attack plans. This type of information could potentially be critical with disrupting a follow-on attack, saving lives, and preserving national security.

This San Bernardino example was a high-profile terrorism related mass shooting. These types of incidents occur much less frequent than strictly violent criminal matters, which occur hundreds of times a day throughout the country. For example, in FBI Director Comey's speech to the Brookings Institution (2014), he provided the following details of the violent murder of a young boy in Louisiana. In March 2010, Brian Horn, a known sex offender, posed as a teenage girl online to lure Justin Bloxom, a twelve-year-old boy, to meet with him (Comey, 2014). On the day of their encounter, Horn, a sexual predator, then posed as a taxi driver, kidnapped and murdered Bloxom. In order to conceal his crimes, Horn attempted to alter and delete electronic data "at rest" on both his and Bloxom's cell phones which was valuable evidence (Comey, 2014). Fortunately, law enforcement was able to legally retrieve the data from both cell phones,

which was critical in linking Horn to Bloxom's murder (Comey, 2014). This evidence was crucial and led to Horn being convicted at trial and being sentenced to death (Comey, 2014). It is safe to assume that if this evidence was encrypted and not able to be retrieved from Horn and Bloxom's cell phones, Horn may not have been found guilty and freed, allowing him to prey on other children.

Data "In Motion" - Terrorist Attack Garland, Texas Case Study

According to a New York Times article written by Rukmini Callimachi (2015), on May 3, 2015, Elton Simpson (hereafter Simpson) and Nadir Soofi (hereafter Soofi), American born Islamic extremists, drove from Arizona to conduct a terrorist attack at the Muhammad Art Exhibit and Contest being held in Garland, Texas (Callimachi, 2015). Wearing body armor and armed with rifles and handgun, Simpson and Soofi drove up to a parked Garland Police Department patrol vehicle at a vehicle access point at the event (Callimachi, 2015). Inside the police vehicle was an armed officer and an unarmed security guard. Simpson and Soofi exited their vehicle and began firing inside the patrol vehicle (Callimachi, 2015). The unarmed security guard was wounded. The armed officer along with nearby responding SWAT officers engaged Simpson and Soofi with gunfire killing them both (Callimachi, 2015).

A Dallas Morning News investigative piece written by Naomi Martin (2017) indicated that prior to the attack, Simpson and Soofi were under FBI investigation because of their suspected extremist beliefs and nexus to terrorism. The FBI was so troubled with Simpson and Soofi's activities they were actively engaging them with an undercover FBI Agent as part of their investigation (Martin, 2017). Additionally, the FBI was so concerned that an FBI Agent was actively surveilling them when the attack occurred. However, a logical assumption can be made that the FBI was unaware Simpson and Soofi were actively planning to attack the event

and lacked the necessary probable cause to arrest them. Subsequent investigation determined Simpson traded 109 end-to-end encrypted messages with a known terrorist overseas on the morning of the attack (Manpearl, 2017). Despite the FBI's concerns with Simpson and his identified connectivity to a known terrorist overseas, they were unable to view the actual communications due to the encrypted messaging applications he was utilizing (Manpearl, 2017). This is a primary example in which law enforcement was unable to view these critical communications and did not possess the technical capabilities to surveil these data "in motion" communications.

As the truly professional and sophisticated terrorist and criminals continue to improve their tradecraft, it can be expected they will increasingly incorporate encryption technologies. This will allow these bad actors a realm to conceal and advance their illicit plans and behaviors which is inaccessible to law enforcement.

Potential Solution

Legislative Options

Despite Director Comey no longer being with the FBI, this debate continues to rage in the public arena. For instance, in 2016 two pieces of federal legislation were introduced, both on completely different ends of the spectrum in this debate. First, the "Encrypt Act of 2016" favored privacy and encryption and prevented any state laws from prohibiting the use of encryption or to compel an entity to develop a design or alter a security function in its product to allow for surveillance or a physical search (House Homeland Security Committee, 2016). Second, the "Compliance with Court Orders Act of 2016" favored law enforcement and required covered entities in possession of a government court order to provide information or data in an intelligible format or provide the technical assistance necessary to obtain the information (House Homeland

Security Committee, 2016). Ultimately, neither piece of legislation was signed into law. However, they are excellent examples as to how divided advocates are on both sides of this debate.

Subsequently, Republican Congressman Michael McCaul and Democratic Senator Mark Werner specifically created the Digital Security Commission, also known as the McCaul/Warner Commission, to bring together experts and representatives from cryptology, global commerce and economics, technology sector, USIC, all levels of law enforcement, and the privacy and civil liberties community (House Homeland Security Committee, 2016). The purpose of this commission was to evaluate the current digital security and encryption challenges and to draft recommendations for Congress to create a comprehensive plan for the future (House Homeland Security Committee, 2016). To date, this commission has failed to issue any type of report or recommendations.

Split Key Encryption

Professor Geoffrey Corn's concept of split key encryption is an innovative solution for lawful access which also incorporates security (Manpearl, 2017). The concept allows for "front door" access to encrypted evidence and intelligence when lawfully authorized, while balancing risks to privacy and security (Corn, 2015). The split key permits the encryption keys to be split and warehoused in separate and distinct locations (Manpearl, 2017). As an added layer of security, the keys themselves can be encrypted (Manpearl, 2017). The theory is the keys would be held by separate entities, such as a technology company and the government. Upon law enforcement obtaining a legal court order, the holders of the keys would coordinate and combine the keys to decrypt the targeted information making it accessible for law enforcement (Manpearl, 2017). By splitting the key, it would become extremely difficult for a cyber hacker or an adversarial nation state to steal both keys and compromise the specified encryption technology

(Manpearl, 2017). It would also make it exceedingly challenging for one of the entities in possession of the keys to abuse it or decipher the encrypted data without the proper legal authority (Corn, 2015). One possible weakness is the split key process is multifaceted and would escalate the complexities of the encryption which could create potential vulnerabilities to be attacked (Manpearl, 2017).

Conclusion – Necessity for Government and Private Sector Collaboration

The "Going Dark" phenomenon is a problem with many complexities which intersect in the privacy vs. security debate. No matter how the decision is made to address "Going Dark" as a society, there will be tradeoffs with positive and negative consequences. For these factors, it is reasonable to suggest a transparent conversation at the national level must occur with all equity holders. In 2016, the creation of the McCaul/Warner Digital Security Commission appeared to be a positive step forward to creating this dialogue. However, three years after its creation, the McCaul/Warner Commission seems to have failed to develop any creative real-world solutions or a path forward. The Obama administration decided against addressing the issue. The current Trump administration is evaluating the issue, but has not developed a strategy to address it. Current FBI Director Christopher Wray has continued the efforts of former FBI Director Comey in being the leading voice for law enforcement concerning the "Going Dark" problem. Director Wray continues to highlight the problem and engage the private sector and legislators to develop practical solutions. Law enforcement agencies, such as the FBI and Department of Homeland Security, understand the necessity for the use of strong and secure encryption by the government and private sector to safeguard our nation and citizens from a wide range of cyber threats. It is in the best interest of law enforcement, who currently employ encryption technologies to secure their networks, data, and communications, to ensure any lawful access requirement does not

create unnecessary vulnerabilities. As previously mentioned, technology companies currently have the capabilities to decrypt data in an easy and secure manner. Building a secure "front door" into encryption technologies appears to be an obtainable goal. Currently, encryption technologies are handcuffing law enforcement from accessing communications and electronic data in circumstances which fall within the legal parameters of the Fourth Amendment and statutory standards. Unfortunately, this places law enforcement at a certain disadvantage from disrupting and solving criminal and terrorist plots and activities.

Legislators have a responsibility to ensure law enforcement has the capacity to conduct reasonable searches and seizures. As a nation, this issue is too critical to ignore and it is essential to provide a level of clarity to all relevant stake holders. In the end, there is a necessity to shed light onto the "Going Dark" problem. Our nation must find the correct balance to preserve individuals' privacy and constitutional rights, while also giving the government the tools to fulfill its greatest responsibility of safeguarding its citizens from evolving threats posed by evil doers.

References

Alhogbani, A. (2015). Going dark: Scratching the surface of government surveillance. *Comm Law Conspectus, 23*(2), 469.

Bennett, C. (2015, July 8,). Administration spars with lawmakers over access to encrypted data. *The Hill.* Retrieved from https://thehill.com/policy/cybersecurity/247228-encryption-battle-reaches-capitol-hill

Callimachi, R. (2015, May 11). Clues on twitter show ties between texas gunman and ISIS network. *The New York Times.* Retrieved from https://www.nytimes.com/2015/05/12/us/twitter-clues-show-ties-between-isis-and-garland-texas-gunman.html

Corn, G. S. (2015). Averting the inherent dangers of "Going Dark": Why congress must require a locked front door to encrypted data. *Washington and Lee Law Review, 72*(3), 1433.

Corn, G. S. (2017). Encryption, asymmetric warfare, and the need for lawful access. *The William and Mary Bill of Rights Journal, 26*(2), 337-360.

Dunlap, C. J. Jr. (2017). Social justice and silicon valley: A perspective on the apple-FBI case and the "going dark" debate. *Connecticut Law Review, 49*(5), 1685.

Federal Bureau of Investigation, Office of Public Affairs. (2014, October 16). *Remarks by FBI director on going dark at the brookings institution.* Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

House Homeland Security Committee Majority Staff Report Committee releases encryption report. (2016, June). *Going dark, going forward: A primer on the encryption debate*. Retrieved from https://www.hsdl.org/?abstract&did=795726

Kerr, O., & Schneier, B. (2018). Encryption workarounds. *The Georgetown Law Journal, 106*(4), 989.

Manpearl, E. (2017). Preventing "going dark": A sober analysis and reasonable solution to preserve security in the encryption debate. *University of Florida Journal of Law and Public Policy, 28*(1), 65.

Martin, N. (2017, May 26,). Security guard injured in garland terror attack tormented by belief that FBI knew of ISIS plot. *The Dallas Morning News.* Retrieved from https://www.dallasnews.com/news/crime/2017/05/26/victim-garland-terror-attack-tormented-belief-fbi-knew-isis-plot

"Mobile fact sheet" Pew Research Center, Washington, D.C. (2018). Retrieved from http://www.pewinternet.org/fact-sheet/mobile/

Posner, S. C. (2016, April). A legal fine point in the apple-FBI dispute. *Privacy Journal, 42*(6), 5.

Potapchuk, J. L. (2016). A second bite at the apple: Federal courts' authority to compel Technical assistance to government agents in accessing encrypted smartphone data under the all writs act. *Boston College Law School Boston College Law Review*, 57(4), 1403.

Schmidt, M. S., & Perez-Pena, R. (2015, December 4). F.B.I. treating san bernardino attack as terrorism case. *The New York Times.* Retrieved from https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html

Schulze, M. (2017). Clipper meets apple vs. FBI—a comparison of the cryptography discourses from 1993 and 2016. *Media and Communication, 5*(1), 54. doi:10.17645/mac.v5i1.805

Senate Select Committee on Intelligence. (2015). *FBI director James Comey's statement "counter intelligence and the challenges of going dark".* Retrieved from https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark

U.S. Const. amend. IV. Retrieved from https://www.congress.gov/content/conan/pdf/GPO-CONAN-2017-10-5.pdf

Zittrain, J. L., Olsen, M. G., O'Brien, D., & Schneier. B. (2016). Don't panic: Making progress on the "going dark" debate. Berkman Center for Internet & Society Publication 2016-1. Retrieved from https://dash.harvard.edu/handle/1/28552576