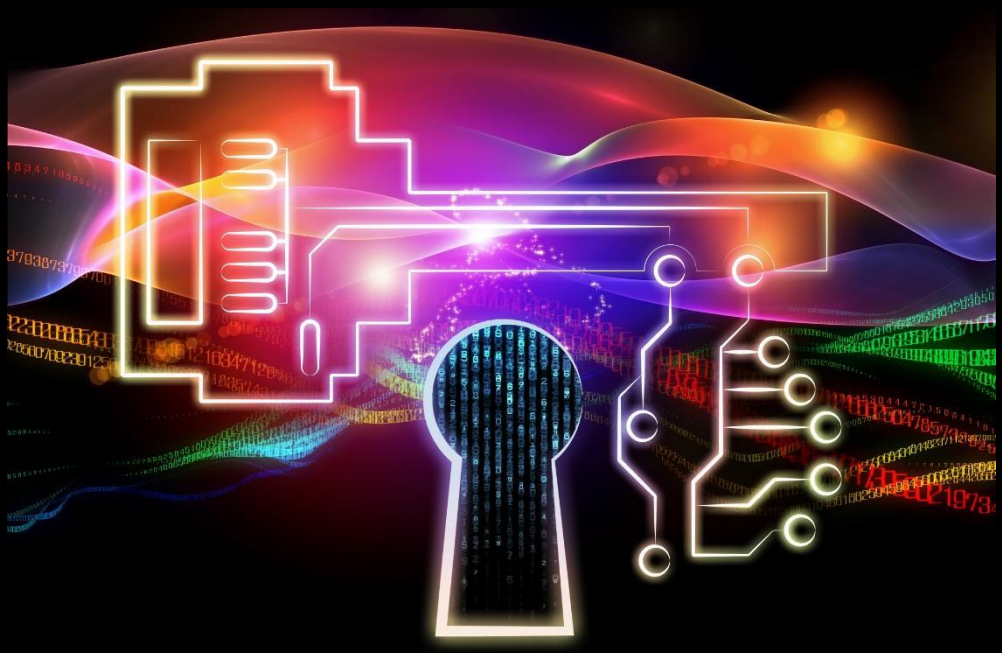

GOING DARK: IMPACT TO INTELLIGENCE AND LAW ENFORCEMENT AND THREAT MITIGATION

Bonnie Mitchell
Krystle Kaul
G. S. McNamara
Michelle Tucker
Jacqueline Hicks
Colin Bliss
Rhonda Ober
Danell Castro
Amber Wells
Catalina Reguerin
Cindy Green-Ortiz
Ken Stavinoha

2017
ANALYTIC EXCHANGE PROGRAM

ACKNOWLEDGEMENTS

We would like to first thank the Office of the Director of National Intelligence (ODNI) for its generous funding and support for our study and learning journey to the DEFCON hacking conference. We are also very grateful to the Department of Homeland Security (DHS) for its support during the duration of the program.

We could not have completed this study without the unwavering support and dedication of Ms. Bonnie Mitchell, ODNI Deputy National Intelligence Manager for the Western Hemisphere and the Homeland, our devoted Team Champion who steered us throughout this study and helped turn an idea into a product.

We would like to acknowledge and thank each member of our public-private sector working group for their tireless efforts from around the U.S., which includes Krystle Kaul, G. S. McNamara, Michelle Tucker, Jacqueline Hicks, Colin Bliss, Rhonda Ober, Danell Castro, Amber Wells, Catalina Reguerin, Cindy Green-Ortiz and Ken Stavinoha.

We are very thankful for all the unique insight we received from interviewees who contributed to this report by educating our group on the many aspects of 'going dark,' and we take full responsibility for any and all errors of fact or interpretation implied or explicit in this paper. Our interviewees include the Village sponsors at DEF CON, private sector industry experts and government officials. We are thankful for the interesting and diverse perspectives particularly from senior government officials and private sector experts. We are very grateful for their time and valuable perspectives on our study topic.

EXECUTIVE SUMMARY

The Department of Justice (DOJ) has publicly noted that the prevalence and sophistication of encryption and the use of new applications (apps) are degrading the ability to collect information pertinent to national security. More specifically, these technologies are diminishing both law enforcement and the Intelligence Community's (IC) ability to lawfully intercept data in motion as well as access stored data. This issue is commonly referred to as the 'going dark'[1] problem. The challenges going dark presents extend beyond the government's requirements. Going dark also touches on privacy issues, technical limitations, legislative shortcomings, and other considerations.

This paper presents the findings of a team of public and private sector analysts focused on the going dark problem and its attempt to collectively address the national security concerns resulting from barriers to data collection. The team arrived at the key findings through extensive qualitative and quantitative research which included conducting interviews on going dark with subject matter experts within the private sector, the intelligence community and law enforcement agencies. It is important to note that the findings, statements, and views expressed in this paper belong solely to the team and do not represent or reflect the position of the U.S. Government or any commercial entity.

The paper puts forth the following policy recommendations and next steps: 1) Broaden the scope of going dark beyond encryption; 2) Look for data beyond signals intelligence (SIGINT) that may contain substantive data; 3) Do not be afraid to hack back; 4) Engage in public discussion on legal protections and solutions; 5) Increase and enhance partnerships across the intelligence community and law enforcement agencies; 6) Increase public-private sector partnerships; and 7) Create government liaison officers tasked to manage relations with both the private sector on specific cybersecurity and privacy issues. These recommendations are intended help the Office of the Director of National Intelligence (ODNI) tackle the going dark problem and help mitigate potential threats with the help from the private sector.

[1] Hereafter 'going dark' will be referred to as going dark.

TABLE OF CONTENTS

INTRODUCTION

The public and private sectors face a growing national security concern resulting from the ability of criminals, terrorists, and state actors to obfuscate their activities by going dark through encryption or other means. Rapidly evolving technological advancements—particularly in digital and communications security— impede the ability of law enforcement and intelligence agencies to collect and analyze information critical to thwarting potential threats. At the same time, strong encryption ensures digital communications are protected for secure commerce and trade, strengthen cybersecurity, and safeguard private information, national security, and the global economy.

Encryption at Rest is an encrypted file system of data and metadata.

Data at Rest refers to inactive data stored physically in data bases, spreadsheets, archives, and tapes. The data is collected from these sources and analyzed after an event or transaction occurs.

Encryption in Transit protects data in-transit between consumers' devices and cloud services

Data in Motion refers to collecting data and analytics in real time as an event or transaction occurs.

Technology continues to advance at a swift pace which provides easier connectivity, accessibility and convenience to all aspects of life. Many Americans rely on connectivity to the cyber world potentially leaving them vulnerable to criminal activity that can jeopardize personal and physical safety. An entire industry offers devices with built-in security mechanisms, data security, decryption and antivirus, and other security protections. These technologies are advanced by industry in anticipation of the public's desire to maintain a certain level of privacy.

Pursuant to federal and state statutes, law enforcement agencies across the country have jurisdictionally specific legal authority to intercept and access communication and information in accordance with court orders. However, the Department of Justice (DOJ) has publicly noted it often lacks the technical ability to carry out those orders due to rapidly evolving advancements in technology, particularly in digital security and communications security. These challenges faced by law enforcement have been collectively termed going dark. The going dark challenges can be broken down into two distinct concerns:

1) Court-ordered interception of **data in motion** is often frustrated by the lack of technical solutions.

2) Law enforcement access to **data at rest** is often limited either by the integration of default privacy measures incorporated into the devices by device manufacturers—in the case of communications records—the lack of data retention standards.

The aim of this paper is to explore the opportunities and challenges for law enforcement and the Intelligence Community that are presented by the prevalence and sophistication of communications and data security. The paper will provide recommendations to update domestic and foreign policies, improve law enforcement tactics and examine solutions to overcome threat intelligence analysis and collection tactics that are hampered by encryption. The overarching goal of the paper is to provide policy considerations, recommendations and next steps to promote public and private sector collaboration that can help both the intelligence community and law enforcement mitigate the threat of going dark.

CURRENT AND FUTURE THREATS

Evolving technological advances present challenges for law enforcement and forensic experts to be able to attribute a certain malicious activity to a specific actor, such as those involving drug trafficking organizations (DTOs), gangs and organized crime, human trafficking, child exploitation, counterterrorism and counterintelligence. The use of encryption and other obfuscation techniques, coupled with the volume of activity, creates a real threat to national security. Below is a summary of the current and future threats related to the going dark problem.

Data at Rest

Mobile phone ownership and usage has grown rapidly over the past six years presenting consistent upward growth in the volume of data available for potential evidence and intelligence analysis by law enforcement and the IC. According to 2017 Pew Research data, 95% of Americans own a cell phone and 77% own a smartphone–the latter figure up from 35% since 2011. A Federal Bureau of Investigation (FBI) regional computer forensics laboratory that tracks the rate mobile phones are examined in cases and has noted an increase of phone 67% annually. Memory card and device storage capacity doubles approximately every 15 months. (Quick, 2017). Smart phone evidence can include call records, GPS data, text messages, emails, photos, and documents. The advent and increasing usage of cloud computing and social media has resulted in smartphone data primarily hosting account information, such as credentials and pointers to documents or photos in the cloud. The phones may only retain cached copies or thumbnails (Martini and Choo, n.d.).

Many technology companies and new operating systems encrypt by default all of a user's information on the user's device. This encryption technology is impossible for even the company (manufacturer) to decrypt data on devices they manufacture and sell even when lawfully ordered to do so. (Hess, 2015) For example, since 2009, several companies have included a dedicated cryptographic chip on its smartphones which enables encryption by default. Files protected with data protection are encrypted with a random file key which is then encrypted using a higher tier class key and stored as a file tag. Passwords (and other sensitive small data) are stored on the device and encrypted using a similar approach. The data is stored in the iOS keychain, a device key escrow mechanism built into the operating system. Files and keychain elements are both protected by one of a number of access control keys which are also encrypted in a way that incorporates the user's device passcode. The passcode must be known in order to decrypt the key hierarchy protecting these select files and keychain elements and also to disable the device's GUI lock (Ayers, 2014).

While a device, such as the iPhone, itself defaults to encryption, many of the apps do not, or they rely on a framework—often Hyper Text Transfer Protocol Secure (HTTPS) over which data is sent between browser and the website to which the user is connected. HTTPS depends on web servers for encryption and can be bypassed. Android devices are not manufactured by a single entity, and thus encryption by default is not broadly implemented on the devices as a whole, but is dependent on the processes of each manufacturer.

Data in Motion

Data in motion is considered to be more vulnerable than data at rest. Encryption in the transmission of information is critical to protect data traveling from one network to another network. Protecting this data is important for individuals as well as businesses and other enterprises to protect privacy and maintain competitiveness.

At the same time, criminals, terrorists, and other adversaries use the same encryption and encrypted service obfuscating their nefarious activity. This usage by bad actors poses a primary challenge to security services: There is no threat actor-specific technology that would allow "back door" access into digital communications that would not also create the risk of a vulnerability in all systems which weakens everyone's security. No longer are enemy communications necessarily on their own network nor on devices and services held specifically by them. The commingling of communications in a globalized world presents an additional challenge requiring an approach more nuanced than a universal backdoor.

The architecture of end-to-end encryption (E2EE) precludes access to the full content even if granted unilateral access by the messaging service provider in compliance with a lawful order. E2EE as a generic design ensures only that the communicating parties possess the information needed to decrypt it, keeping any messaging service provider or intermediate party out of the loop. But increasingly, privacy-conscious communications tools are rolling out a feature known as end-to-end encryption. That end-to-end promise means that messages are encrypted in a way that allows only the unique recipient of a message to decrypt it, and not anyone in between. In other words, only the endpoint computers hold the cryptographic keys, and the company's server acts as an illiterate messenger, passing along messages that it can't itself decipher" (Greenberg, 2014). The use of end-to-end encryption presents a challenge for access to the content itself requiring innovation instead in the avenues of metadata analysis and endpoint compromise.

Hiding in Plain Sight

Going dark is more than just encryption. It can be as simple as hiding in plain sight in order to conceal one's identity and internet activity. Individuals may use a number of easily available and often free tools to conceal or misrepresent their physical location and anonymize their online activity. Some hurdles for law enforcement and forensic experts include strong E2EE limits on data retention, legal binds on U.S.-based services and companies' technological capabilities which may include providing information to law enforcement through legal processes such as subscriber information that could identify and locate users online. This landscape consists of mixed wireless, cellular and other networks through which individuals and information are constantly passing and tools facilitating anonymity (International Association of Chiefs of Police, Data, Privacy, and Public Safety, 2015) (Testimony before U.S. Congress, 2016). A logical progression of these actors is to migrate to the Dark Web where there is a greater perceived notion of security and anonymity.

The Onion Router (Tor)[2] is a software tool that anonymizes activity by bouncing encrypted information between multiple computers or "relays" before the information reaches its destination. (Tor Project: Anonymity Online, n.d.) (Service, 2017) Tor is not merely a proxy chain[3], but an onion router, which means that routing information—as well as message content—is encrypted in such a way as to prevent linking the origin and destination. Similar to all anonymity networks, the Tor network cannot 'end-to-end' encrypt messages destined for the public Internet. This must be arranged between the sender and recipient. Tor's hidden services such as Silk Road, AlphaBay, Cryptocat and The Magic Kingdom do provide E2EE along with the ability to anonymize servers to make them more censorship-resistant.

---

[2] The Onion Router (Tor) provides anonymous communications by directing internet traffic through a free, worldwide, volunteer network to disguise the user's location and usage. Tor encrypts the user's data, including their Internet Protocol (IP) address and passes the data through multiple 'relay' nodes until it reaches the exit node. The exit node decrypts the user's data and sends it to the destination website. The website thus views the user as accessing the site from the exit node.

[3] Proxies can be daisy chained. Chaining anonymous proxies can make traffic analysis far more complex and costly by requiring the eavesdropper to be able to monitor different parts of the Internet. An anonymizing remailer can use this concept by relaying a message to another remailer, and eventually to its destination.

Evolving technological advances presents a set of opportunities for law enforcement and forensics experts in developing ways to bypass anonymity protections of software such as Tor and attribute certain criminal activity to a specific actor(s). Some examples include:

- Through the development and diligence of Network Investigative Techniques (NITs), the FBI reportedly seized the server hosting a large child pornography forum on the Dark Web in early 2015. It then ran the site from its own servers and used an NIT to identify individuals frequenting certain portions of the site (Jeong, 2016).

- In 2013, the FBI reportedly took control of Freedom Hosting—a website hosting service operating on the Tor network and reportedly home to more than forty child pornography websites—and infected it with "custom malware designed to identify visitors." (Jeong, 2016).

The Invisible Internet Project (I2P) is a means to use strictly message-based anonymous, highly dynamic and completely decentralized network for internet communications and browsing whereby a routing user's I2P can remain end-to-end encrypted (in total there are four layers of encryption used when sending a message). The end points are cryptographic identifiers and will never show on public websites' logs. Although Tor and I2P serve a similar purpose, I2P can be used to navigate Internet Relay Chat (IRC) networks which ban Tor users and is a fully internal anonymous network. The philosophy behind I2P is that each node routes traffic for others and blends its own traffic in, whereas one's own traffic will be relayed by other peers through so-called tunnels made up of various other peers.

Another example, the Virtual Private Network (VPN) Individual Internet is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols or traffic encryption. From a user's perspective, the resources available within the private network can be accessed remotely and a user may secure their wireless transactions with a VPN to circumvent geo-restrictions and censorship or to connect to proxy servers for the purpose of protecting personal identity and location. However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions and have been banned in countries such as China and Russia.

The sole use of an anonymizer such as, Tor, I2P, and VPN is one way of hiding in plain sight, but it is not the only method. An alternative method is through the creation of an alter ego for non-encrypted applications such as Facebook, Twitter, Instagram, and Google. This alter ego can be used in conjunction with an anonymizer. There are a number of websites that provide tutorials and guidance on the successful use of this alternative method which includes obtaining virtual phone numbers, creating multiple unique email addresses, browsing in private mode, and using Tor or a VPN service to obscure the user's true IP (Internet Protocol) address and location.

AGGREGATION OF EXISTING SOLUTIONS AND OPPORTUNITIES

The intelligence community and law enforcement are actively working to discover methods to access data at rest and data in transit. Based on independent research and discussions with subject matter experts, technical solutions may exist to access encrypted data, but further exploration is needed. Independent research also notes a growing interest in legislative measures to address aspects of the going dark problem. Below is a brief summary of technical solutions and non-technical opportunities to assist law enforcement with the going dark problem.

Brute Force Decryption

The most aggressive form of an encryption breach is a "brute force" attack; the attempt to decrypt by trying a wide range of possible solutions to the algorithm used to create the encryption. In 2012, researchers discovered that a less-than- eight character Windows password could be compromised via brute force in six hours (Knight, 2012). More sophisticated passwords and the implementation of technology like "CAPCHA" have had relative success in thwarting such attacks.

Even complex cryptographic systems such as Advanced Encryption Standard (AES) potentially face the possibility of exploit resulting from the evolving sophistication of attacks coupled with the growing computing capabilities. Quantum computing will change the encryption landscape, but it is not yet clear how much it will change. It is not clear because we are not yet certain what sorts of problems quantum computers can solve—not all cryptographic routines are known as weak vs. quantum computing. However, with quantum computing also lies the ability to 'quantum' encrypt which levels the playing field between encrypting and decrypting.

At a tactical level there is an opportunity to exploit deprecated low-strength encryption even in the face of improvements in the field. Industry has shown to lag years behind the implementation of the newest and strongest encryption standards as older ones are proven vulnerable by the security research community. For instance, the first practical attack on the MD5 cryptographic algorithm upon which much of Web communication relied for encryption was conducted in 1996 (Dobbertin, 1996), but only in 2011 did Google Chrome¯one of the most popular Web browsers—begin to cease support for the weak algorithm (Sleevi, 2011).

Additionally, a few large industry players such as Facebook and Cloudflare have supported both a new and more robust encryption standard as well as an old vulnerable one as a fallback for customers on older devices. In this case, this leaves a known attack vector in place for up to 7% of the Internet's users (Goodin, 2015). This is a unique opportunity for foreign intelligence gathering as a disproportionate number of these older devices exist in developing countries.

Interception of Encryption

One area of vulnerability that is increasingly becoming a focus of the security community is the ability to attack early in the development of products and services—the supply chain. Attacks here can undermine encryption from the beginning. Due to the confluence of factors such as the urge to reduce costs in order to beat competition, the vendor sourcing subcomponents from multiple other vendors and with little oversight into the organization's security and facility itself, this vector is prime for successful exploit in both the short and long-term.

When considering attacks on the overall software supply chain it is now common that "[d]evelopers are a prime target for attackers, as they often use [a] less secure environment, are administrators on their own systems and have access to sensitive information" (Cherny and Dulce, 2017). The impact of a successful attack is such that "[a] single developer infected could affect the entire production pipeline" (Cherny and Dulce, 2017). This reality is compounded by the fact that there may not be much oversight into the development shops—many of which are startups—in terms of tackling questions such as: 1) who are the developers? 2) where does the development actually take place? and 3) how to vet re-used software modules?

When the objective is to embed code on a target device it is significant to note that some software manufacturers do not sign their software updates, allowing for the possibility of breaching devices via malicious updates. For those that do sign their code, crafty criminal groups have taken to stealing code-

signing certificates from the manufacturers themselves so that these groups can sign their malicious software updates to appear legitimate (Microsoft, n.d.). This attack vector is not limited to malicious updates of legitimate software, but also to entire hacking tools and pieces of malware to be installed on a compromised target device (DiMaggio, 2016).

The delivery mechanism not only on software, but also on the data ingested by intelligence-driven products—whether security in nature or not—is a possible exploit opportunity. Similar to the unsigned code problem intelligence feeds directing software to take action or to look for certain indicators of malicious activity can be tricked into inaction by manipulating the ingested feed so that it does not have the information it needs which leads to false negatives. In this instance, attacks might subsequently go unnoticed. These are some of the possibilities when considering attacks on the supply chain and how they can lead to compromising technology directly or undermining it by cutting off the intended information it depends on to operate.

Certificate Management

Today's digital environment is highly dependent upon Secure Sockets Layer (SSL)/Transport Layer Security (TLS) certificates. "Certificates allow machines to communicate securely and that makes them an essential, but underappreciated, part of every organization's digital ecosystem and our global digital economy" stated Kevin Bocek, Vice President of security strategy and threat intelligence at Venafi (Masters, 2017). According to a study conducted by Dimensional Research in 2016, 79% of the businesses surveyed had suffered at least one certificate related outage last year. Some prominent certificate issues that made headlines in recent years are:

2013: Microsoft Azure outage due to an expired certificate lasting nearly a day (Expired SSL Certificates: How Is This Still a Thing?, 2015)

2013: Partly due to US Government shutdown, approximately 200 .gov websites were using expired certificates (Duncan, 2013)

2015: Expired Google certificates interrupted its Gmail service (Expired SSL Certificates: How Is This Still a Thing?, 2015)

2017: Kaspersky bug disabled certificate validation for 400 million users (Chirgwin, 2017)

2017: Google and Mozilla engineers discover that Symantec improperly issued 30,000 certificates (Cimpanu, 2017)

Expired certificates provide opportunities for compromise. Web browsers differ widely in the treatment and notification of invalid certificates. When an SSL error occurs some browsers only display a single error message sometimes not the most serious or even a generic error message for all types of SSL errors. An attacker can exploit this vulnerable browser behavior on SSL sites with expired certificates to perform an almost seamless man-in-the-middle attack. By signing his/her own expired SSL certificate for a U.S. government website, the SSL error message displayed for the attacker's SSL certificate is indistinguishable (in some browsers) from the error message produced by the real SSL certificate belonging to the U.S. Government. Citizens accustomed to seeing the "expired" error message will happily proceed with a connection using the attacker's expired and untrusted certificate unwittingly communicating with the attacker instead of the U.S. Government (Duncan, 2013).

Certificate management, or lack thereof, is a major issue in the going dark debate. The Dimensional Research study found that 65% of businesses do not centrally manage certificates and of the businesses that do two-thirds depend on security controls from a third party Certificate Authority (e.g., Symantec), which limits the visibility of the business into the certificates. Most businesses surveyed did not have automated processes for managing certificates nor have an effective tracking system for expiration of the same certificates.

Aggravating the situation is the magnitude of devices needing trusted interactions. The Internet of Things (IoT) is adding billions of connected devices that could overwhelm an already dire situation. To help remedy the situation Qualys announced on July 24, 2017 that its CertView application will catalog and improve the visibility of any security certificates issued by certificate authorities (Osborne, 2017).

Traffic Analysis and Metadata

In cases where extraordinary access and content inspection are not possible through acquisition via signals intelligence (SIGINT), the government may focus on the possible value derived from metadata. As encryption is implemented in an expanding number of ways, a focus on metadata should intensify should brute force attempts to break encryption prove impossible.

"In the future, intelligence services might use the Internet of Things (loT) for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials" (Clapper, 2016). IoT links objects to the Internet, enabling data and insights not available before (CISCO). Corporations house a trove of personal data that will only grow with the expansion of technology. These enterprising entities are interested in ways to monetize the data further and perhaps could offer it for sale to the government at some point in the future to increase sales and company valuations prior to an acquisition. This is an interesting avenue to the data that is worthy of further consideration.

Metadata is useful not only after the fact--after communications might have taken place--but proactively to judge intent of the adversary. In a presentation by Peyton "Foofus" Engel, an Attorney at Hurley, Burish & Stanton, S.C. titled "Secret Tools: Learning about Government Surveillance Software You Can't Ever See" at the July 2017 DEF CON 25 hacking conference (Engel, 2017), Peyton spoke about law enforcement's use of Tracker Messages to discover who is interested in particular content on a peer-to-peer sharing network. The content of interest to law enforcement is of course that which is illegal to possess and the intended procurement evinced by the signature of the particular piece of content in its metadata is valuable when initiating or furthering an investigation. Further, we learned that another feature in peer-to-peer sharing is Torrent Segment Data whereby "peers announce what pieces of files they possess, when they connect for downloads and when they acquire new segments." Effectively, this is a declaration of content possession and willingness to distribute.

There exists an opportunity with metadata to educate the public in a political and cultural sense on what it is and how it differs from content inspection. Currently, signals intelligence is characterized by electronic items which have strict rules about what can and cannot be collected and then once acquired by the IC can be accessed in any manner. Some IC agencies are able to collect metadata, but not content of telephone calls or emails. There are strict rules about when metadata can be viewed which challenges the traditional model and opens the debate to new ways of thinking about how to access data (Brenner and Martin, 2014).

The new reality might be that in the face of strong encryption, protecting message content is necessary to leverage the ability to collect and analyze metadata more than before and to be aware of new challenges that it may present such as handling scale and falsified metadata meant to obscure and misdirect

the government's investigative efforts. The technology revolution and availability of information to law enforcement may represent an anomaly and the implementation of encryption could mark the return to the status quo ante, where access to this data is more limited, according to one former government official (Sinclair, 2016).

Backdoors

A major point of contention in the going dark debate is whether or not companies should build in an access mechanism for the government. Exceptional accesses—commonly referred to as "backdoors"—are intended to provide the government with a method to access secure information and communications systems. The issue of enabling backdoors has persisted in the national debate for many years although the intensity of the debate has accelerated because of technological advances and unauthorized leaks about government surveillance programs.

Advanced communications technologies increased in the early 1990s along with the development of commercial encryption products. The National Security Agency (NSA) was particularly worried about the potential loss of criminal and terrorist telephone communications because of these products. In response, the agency developed an encryption device that would protect personal communications and provide a backdoor for the government to gain entry to that information. (Gallagher, 2015). The Clipper chip was an effort initiated by the White House to balance law enforcement and national security requirements with privacy and other commercial interests. The Clipper chip maintained the ability for two parties to communicate in private via encryption in which each of the two parties has a unique digital key that allows them to decipher the communication. However, with a court order, the Clipper chip was intended to provide the government with wiretap access to the communications by operating on a concept called "key escrow." Essentially, a third key would be created at the time the cryptologic equipment was manufactured and held in escrow by the government. It was to be used when necessary and in a manner that was consistent with the law. In order to incentivize companies to adopt the Clipper chip, the government offered to loosen export controls on encryption products that incorporated the Clipper's key escrow. At the time, the export of encryption tools were subject to strict controls. The government ended up leveraging the controls since it could not mandate specific encryption standards (Gallagher, 2015).

The debut of the Clipper chip sparked intense debate among government, civil liberties groups, and technologists. Supporters contended that it provided a compromise between security and privacy. Opponents of the Clipper chip argued that it suffered from various technical vulnerabilities which would result in more harm than good as they could be exploited for nefarious purposes. They also claimed that those who wanted to hide their conversations from the government could do so through relatively simple methods that circumvented the Clipper chip's capabilities such as adding a layer of encryption before the Clipper chip's encryption. Along these lines, the Clipper chip would only enable the government to surveil those who did not care if the government did so. Further, it was argued that the Clipper chip would provide significant challenges for private industry to compete internationally (Gallagher. 2015). Finally, the Clipper chip was seen as an effort by the government to regulate and mandate an encryption standard, essentially sanctioning the use of other encryption algorithms. In doing so, it was argued that this would have the unintended consequences of further driving the development and adoption of other encryption algorithms by criminals, terrorists, and people that generally did not want to be susceptible to government surveillance.

The technical limitations of the Clipper chip—and more broadly key escrow and trusted third party encryption—results in other significant risks and issues. By providing a third key to the government and effectively concentrating decryption information in one place, it makes it an extremely high-value target for adversaries. As the Office of Personnel Management (OPM) data breach demonstrated, having vast amounts extremely sensitive information located in one place presents an enormous risk. Although the

government is attempting to better secure its information systems, other incidents have demonstrated that the human aspect is another element that is rife with risk. Management of a third key system would require an enormous amount of trust. As the Snowden leaks have demonstrated, a determined individual with an agenda can abuse that trust and cause irreparable damage.

In addition, such a system would require enormous resources to manage and operate, which would be compounded by the ever-growing number of encrypted applications and devices worldwide. Such a system would not only be extremely costly and impractical, but it would also be extremely complex. The more complex a system is, the more it becomes difficult to detect vulnerabilities and flaws (Abelson, 2015).

Ultimately, the Clipper chip program was scrapped in 1996 though the same arguments for and against incorporating backdoors have persisted to today. The debate was renewed in part by the December 2015 terrorist attack in San Bernardino, California, which propelled the issue of going dark into the limelight and on the international stage. Then FBI director James Comey maintained that ubiquitous encryption has significantly hampered the ability of law enforcement and the IC to lawfully access stored data and intercept communications. Subsequently, technology companies have continued to respond to consumer demand for secure communications by providing advanced services and features such as E2EE (Kassner, 2015).

Comey has surmised that technology companies could develop a solution that would enable government access that does not weaken security. He offered that the limiting factor was their business models rather than a technical one (Comey, 2015). Companies are now using encryption as a selling point, marketing it in response to the leaks (Comey, 2014). One solution that has been posed—often referred to as a "front door" such as customizing encryption solutions for law enforcement or legislation that calls for companies involved in telecommunications to design their equipment and services in a way that allows federal agencies to monitor communications, has been argued by Comey that it could achieve both needs although security researchers contend that it is fundamentally not possible with E2EE.

Beyond backdoors, there are several other ways in which the government can access secure communications and data. There are vulnerabilities that can be exploited such as zero-days as the FBI demonstrated in the San Bernardino case where it successfully accessed data on a locked device. However, that calls into question whether or not the government has a responsibility to report zero-days to private companies. It is a dilemma for the government because if the vulnerability is revealed, the market would respond quickly to remedy the vulnerability either through technical correction of the existing product or service or by creating an entirely new product, service, or technology.

Legal

The basis for government warrants on electronic data is derived from the Electronic Communications Privacy Act of 1986, specifically the Stored Communications Act (SCA). This was passed to expand Fourth Amendment protections to individuals against potential intrusions on their privacy arising from illicit access to stored communications in remote computing operations and large data repositories that store e-mail. The SCA empowers the government to compel a provider to disclose customer information and records (Government Publishing Office, 1986).

Recently two cases have highlighted the complex nature of this topic illustrating that U.S. courts do not agree on the interpretations of certain provisions in current law. In each case, the DOJ possesses legal orders to compel Microsoft and Google to return data on U.S. person information. In both cases, the companies have provided data stored from identified individuals to the government, however, neither company has returned data from company servers overseas.

In Microsoft's case, an appellate court found that Microsoft did not have to provide data that resided on their servers in Ireland because the original judge who signed the warrant was not within the legal jurisdiction to do so (Microsoft, 2016). The Second Circuit explained its decision, "when interpreting the laws of the United States, we presume that legislation of Congress is meant to apply only within the territorial jurisdiction of the United States...The court further explained that 'a court must evaluate whether language in the relevant act indicates a congressional purpose to extend the coverage of such an act beyond places over which the United States has sovereignty or some measure of legislative control.'" (Microsoft, 2016). Ultimately, the Second Court found that the SCA focused on user privacy and that forcing Microsoft to provide user communications stored in Ireland would be an unlawful extraterritorial application.

In Google's case, the appellate court ruled that Google had to provide all data regardless of the servers' location (United States District Court for the Eastern District of Pennsylvania, 2017). In this case, the crux of the issue is more complex because of the manner in which Google stores and transmits users' data. According to Google, some user files may be broken into component parts and different parts of a single file may be stored in different locations—and, accordingly, different countries—at the same time. The data is automatically moved from one location to another as frequently as needed to optimize performance, reliability and efficiencies. As such, Google contends that it does not currently have the capability, for all of its services to determine the location of the data and produce the data to a human user at any particular point in time. Google argued that the warrant that was issued only applied to U.S. data and that the government could not compel Google to produce records that are, or may be, stored outside of the U.S. based on the Microsoft ruling. Under the Microsoft ruling, a warrant under the SCA "lawfully reaches only data stored within the United States" (Microsoft 2016). Prior to the Microsoft ruling, Google routinely complied with federal court search warrants and produced data located on servers overseas.

According to the appellate court, at the heart of the Google case are Fourth Amendment protections, which protect two types of privacy expectations: one involving 'searches' the other 'seizures.'" "A 'search' occurs when a reasonable expectation of privacy is infringed." "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessor interests in that property.' The judge contended that electronically transferring data without a user's knowledge does not amount to a "seizure" because it does not interfere with the customers' access or possessory interest in the user data (United States District Court for the Eastern District of Pennsylvania, 2017). Also, the Microsoft case differs from the Google case because in Google's case the data location could change from the time the government applies for legal process to the time when the process is served upon Google. Therefore, it would be impossible for the government to obtain the sought-after user data before the data could be moved. As a result, the judge ruled Google was compelled to provide all user data within the scope of the warrant regardless of where the data was stored.

These judicial rulings have led several legal analysts to believe that these cases should be decided by the Supreme Court as the Fourth Amendment is at the heart of these discussions. What has not been discussed yet, is the ever growing industry of the "Internet of Things" and the items that store and transmit data to third party companies. Enormous amounts of data are transmitted to third party companies. The data is then linked with other collected data, creating more comprehensive records about an individual. Those records are then sold to other parties and the cycle repeats. The records are stored indefinitely and all of this occurs routinely without the individual consent. The reason is because individuals, as consumers and product users, have little choice in the matter. The tradeoff for the conveniences that technology provides is that the user must allow companies to collect their data (Harvard Law Review, 2017).

PUBLIC'S DYNAMIC SENTIMENT

In addition to addressing the technical and legal aspects of the going dark problem, public opinion appears conflicted between advocating for personal privacy and supporting tactics to decrypt or collect data in the interest of national security. Discussions with subject matter experts indicate that a public awareness campaign would assist to communicate the ongoing national security need and potentially garner public support for increased collaboration between the intelligence and law enforcement communities and the technology industry. Below are our findings on public opinion and a potential method to shape it in favor of support toward the intelligence and law enforcement communities.

Public Opinion Regarding Collection

The conflict of digital security, encryption, and civil liberties was addressed through the 2015 USA Freedom Act legislative reform. This was an incremental policy change in response to the 2002 Patriot Act based on expert and political input in which bipartisan support and coalition building with major technology companies resulted in agreement to narrow certain government surveillance programs. However, the digital encryption and privacy policy issue again gained notable public and political salience after the San Bernardino case. The Apple-FBI conflict furthered the divide between law enforcement agencies and the technology sector's data sharing compliance regarding privacy. Through this course of action, institutional fragmentation among states, as well as federal opinion, became evident as contradictory legal rulings of All Writs Act (AWA)[4] interpretation did not render a definitive outcome.

In a Pew Research Center survey conducted in 2016, 51% of Americans felt that Apple should be required to unlock the iPhone at the FBI's request, while 38% felt that Apple is not required to do this. This survey posed a broader question with two competing statements about the tradeoffs between security and privacy and the finding was that Americans' views on this subject remain divided. Forty six percent of Americans agreed with the statement, "The government should be able to access encrypted communications when investigating crimes." A comparable 44% believed that "technology companies should be able to use encryption technology that is unbreakable, even to law enforcement." An additional 4% of Americans volunteered that their answer to this question depends on the circumstances. There is also a partisan element to these views. Democrats, including independents who lean towards the Democratic party tend to support the notion that technology companies should be able to use encryption protocols that are unbreakable to law enforcement. Meanwhile, Republicans tend to feel more strongly that the government should be able to access encrypted messages when investigating crimes by a 53% to 38% margin (Maniam, n.d.).

Is the public's sentiment influenced by disasters, perhaps those of a large scale (e.g. 9/11)?

In the wake of a large-scale disaster, public perception appears to be more readily influenced by symbolic attempts of policy making and not on a technical, expert-driven foundation. Collective public education of the use of privately and publicly collected data must be improved to promote and identify opportunities in the policy realm to simultaneously secure the public's data while aiding comprehensive

[4] The Power to Issue Writs: The Act of 1789 or All Writs Act was utilized by the FBI used as its legal order in its effort to secure Apple's cooperation to access the phone of the San Bernardino attacker. The act authorizes the US federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." (http://constitution.findlaw.com/article3/annotation06.html)

reform to the government's ability to collect information for law enforcement purposes – not as a reactive decision to a large scale event.

In the policy arena, major events in which the public's sentiment is influenced are referred to as focusing events or sudden shocks to policy systems that rapidly increase attention to a suddenly revealed problem. In the streams approach, a focusing event opens windows of opportunity because events provide an urgent, symbolic example of claimed policy failure (Birkland, 1997). The 2001 USA PATRIOT Act illustrates how surveillance policy reform, previously a controversial issue, was viewed as an urgent response to the September 11, 2001 (9/11) terrorist attacks. This major event prompted a quick passage of major policy reform related to government surveillance as the 9/11 attacks dominated the public's attention and helped reset the policy agenda for uncontested policy response.

More recently, "the Islamic State's impressive social media efforts, including through encrypted communications, have enabled it to reach larger audiences across a wider span of the world and to secretly mobilize "lone wolves" to attack in the West. Many of these individuals will have had little or no direct contact with the Islamic State as an organization." (Byman, 2015). Indicators such as the transfer of materials or money may no longer exist for modern attacks that are low-budget and spring from an idea transferred over one of many possible mediums, protected by encryption.

At the same time, more than three-quarters of Americans doubt the nation's ability to stop "lone wolf" terrorist attacks by individuals acting on their own, according to a Washington Post-ABC News poll (Clement, 2015). According to the same survey, Americans have greater confidence in the nation's ability to prevent terrorist acts that are of a large-scale and logistically more complex.

This symbolic pathway for policy reform is at odds with the expert driven approach to the highly technical encryption policy conversation in which incremental changes are advocated given the complexity of the issue. Advocacy coalitions from a variety of positions (e.g., elected and agency officials, interest group leaders, researchers) shape the particular belief system–a set of basic values, causal assumptions and problem perceptions—and exemplify a significant degree of coordinated activity over time. Advocacy coalitions use belief systems rather than interests as beliefs are more inclusive and verifiable through questionnaires and content analysis (Sabatier, 1998).

To ensure the sustainability of technology policy related to encryption, it is reliant on superseding public sentiment, through public education related to a basic understanding of cyber-technology, data collection, and self-policed cyber hygiene. In 2015 and 2016, Pew Research Center surveys explore the issues of the public's attitude regarding privacy, security, and surveillance and place them in the wider context of the tracking and profiling that occurs in commercial arenas. The surveys find that Americans feel privacy is important in their daily lives, but that they recognize they are under surveillance when in public and with little control over the data that is collected about them and how it is used. Adding to earlier Pew Research reports that have documented low levels of trust in sectors that Americans associate with data collection and monitoring, updated findings show Americans also have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions. (Madden and Rainie, 2015). Americans express a consistent lack of confidence about the security of everyday communication channels and the organizations that control them—particularly when it comes to the use of online tools. However, many Americans struggle to understand the nature and scope of collected data and exhibit a lack of faith in organizations, public or private, in protecting the personal information collected. Due to a lack of legislative driven policy or regulation, data retention policy is primarily left to a company's terms and conditions, criticized as the "surveillance business model (Rashid, 2014) in the marketplace, where the benefit of stored collected data can be used for purposes outside the scope of the original collect, introducing vulnerability of large data sets to be hacked or exploited (Bowdish, 2015).

When it comes to their own role in managing personal information, most adults were not sure what information is being collected or how. Half those surveyed said they felt confident that they understood how their information would be used, 47% said they were not. Many of these surveyed felt "confused", "discouraged, or "impatient" when trying to make decisions about sharing personal information with companies. 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies (Rainie, 2016).

Is Transparency Another Influencing Factor?

The issue of transparency has been injected into the public going dark debate by the Snowden leaks and other unauthorized disclosures (Gellman, 2014) (Barrett, 2017). How does the government address the issue when the very nature of surveillance and intelligence collection generally require varying levels of opacity that are dependent on several factors? Sources and methods, vigilance of the target, as well as the sensitivity of an operation and its intended outcome, all factor into the equation. The ability to play offense while simultaneously playing defense in the digital world is extremely difficult. The public expects the government to exploit vulnerabilities in order to manage our nation's adversaries. At the same time, the public likely expects the government to protect us from the same vulnerabilities. The public also expects the private sector to protect us from such vulnerabilities. As such, the ongoing leaks about government surveillance tools and methods have, and will continue, to prompt companies to correct their vulnerabilities. Though leaks are not an intended method of transparency, they may have the same effect as government efforts to be more transparent.

Not only can transparency provide accountability, but it can also provide the public with information in which they can better understand and engage in public discourse. Public discourse provides an opportunity for transparency, and it is strengthened when it allows experts from all sides to weigh in. The concerns of each are very real and serve to shape the debate. This group observed a lack of presence by representatives from the intelligence and law enforcement communities during a research trip to DEF CON 25 in July 2017. DEF CON promotes itself as the premier hacking conference, and it is attended annually by thousands of digital security professionals, researchers, students, lawyers, and "techies" among others. The conference features numerous presentations and panel discussions, which allow for interaction among the attendees. Although the conference has had a somewhat contentious history with intelligence and law enforcement, the group was surprised when a former intelligence community professional who was presenting received a resounding applause from the audience when he acknowledged that the intelligence community was working very hard to preserve democracy and protect their freedoms. Following his presentation, he was surrounded by a crowd of people wanting to thank him and engage in more discussion with him. Clearly there is an earnest desire for more dialogue. The government and private sector should take advantage of opportunities to engage and dialogue with the public. Conferences such as DEF CON provide a unique forum where all sides can express their concerns, challenges, successes, and failures. The government should be as open as possible in these engagements, with the intent to not only inform, but also to learn. As in the case of DEF CON, who better is there to engage than those with a passion for accessing systems that are designed not be accessed?

Transparency doesn't necessarily have to include how the government is conducting surveillance. Instead, the government can shed light by continuing to provide real-world examples of the challenges it faces. In essence, it may need to market its failures to clearly demonstrate the challenges. However, revealing failures may exacerbate the problem by pointing out weaknesses and limitations in capabilities that criminals and terrorists can capitalize on. Conversely, the government may or may not be able to provide real-world examples of successes it has had. The government is hampered in its ability to do so because of the possibility to reveal sources and methods. Doing so may result in the changing of technology trends, algorithms, or the correction of vulnerabilities. It could also cause backlash and reduced cooperation

among private sector companies who do not want consumers to know that they cooperate with, or facilitate, government surveillance, particularly as privacy solutions are a profitable commodity (Gregg, 2016).

Psychographic Segmentation – Fostering the Public's Trust of Government through Personalized Messaging

Psychographic segmentation entails better understanding one's audience based on personality traits, interests, attitudes, opinions, and lifestyle. This defined segment is then utilized to develop and tailor-focus messages that more strongly resonate with the targeted grouping. By analyzing and applying beliefs, interests, and principles, such messaging engages an audience in ways that persuade or even influence a person because they appeal to the individual on a personalized, value-based platform. The added significance of psychographic segmentation includes that it surpasses what utilizing demographic segmentation alone would miss. If an individual's desires could be understood on a basis more personal than where they live but rather what their beliefs are, then solutions or reasoning for approaching a person in a certain manner are better known. Demographics do not provide the reasons for why decisions (or purchases) are made, as they simply define what age groups, geographies, genders, etc. happen to correlate with or agree or disagree with certain values. According to Alexandra Samuel of the Harvard Business Review, online communities enable marketers to consolidate psychographic differences by leading people to identify more with groups sharing a common interest or value, rather than by geographic or demographic similarities. In turn, psychographic data acts as a "roadmap for navigating divisions and sensitivities" between values as the reasons for harboring certain attitudes become more clear (Samuel, 2016).

Regarding public opinion on government surveillance and the use of encryption technology, it was discovered that the division between supporters of government surveillance and encryption technology bans and opponents of these may be derived and defined at a highly personal, psychographic level. Chris Sumner of the Online Privacy Foundation found that individual personality traits play a strong role in determining individual sentiments toward government surveillance; specifically, that these viewpoints are influenced by a person's level of authoritarian or non-authoritarian tendencies. Sumner concluded that individuals with an authoritarian disposition were more likely to be supportive of government surveillance and bans for counter-surveillance technology while those with non-authoritarian backgrounds were less likely to be in support of these views. Moreover, perception of imminent threat of terrorism was discovered to be a catalyzing factor in accelerating the probability of support for government surveillance. Utilizing data generated through surveys of U.K. citizens regarding the Charlie Hebdo terrorist attacks of 2015, the Online Privacy found in a recent study that perceived threat increased the probability of support for government surveillance, even among individuals who were lower in authoritarianism. Furthermore, individuals who were deemed less authoritarian became increasingly supportive of surveillance the greater their perception of the threat of terrorism – almost to the point of equalizing and surpassing percentages of support by more authoritarian individuals. Throughout the study Sumner found that persuasiveness of ads does work, yet postulated that challenging misleading information is difficult because peoples' ability to interpret evidence becomes more difficult if it goes against their existing beliefs. Finally, Sumner found that people tend to have a greater attention span for ads that utilize fear as a tactic (Sumner, 2017). These findings highlight that it is increasingly important to know the target audience and tailor a message appropriately to what the audience will respond to positively and even shift their existing beliefs.

A direct application of psychographic targeting would be in aiming to debunk the misconception that the government is interested in either banning encryption technology or utilizing key escrows or backdoors in order to mitigate the issue of going dark. Aside from a direct press release, public statement, or grassroots level educational engagement, psychographic targeting would enable scaling of focused advertisements to be targeted at individuals who, based on their interests, values, personality, would be more likely to oppose government surveillance or, even further, believe that the government is pursuing

key escrow. The idea would be to erode or even shift the individual's existing belief in order for trust to begin to build at a micro level.

Therefore, it is posited that a better understanding of the wider public in terms of interests, attitudes, behavior and personal values, psychographic segmentation and targeting would enable the messaging of pro-government trust and surveillance stances to be more nuanced in such a way that the messaging resonates in an impactful way with targeted audiences. In order to advocate for increased trust, the following steps should be utilized for employing psychographic segmentation and targeting as a supplemental 'marketing' or public relations strategy:

- Research the psychographic feelings, values, and interests correlating with pro-government and anti-government sentiments.
- Understand if certain values resonate with support for government surveillance, comparing results with the Online Privacy Foundation's findings regarding authoritarian personalities.
- Understand more comprehensively what values resonate with anti-government surveillance sentiments. If strong privacy is an associated value or argument, further define psychographic profiles for individuals with this view.
- Understand baseline levels of perceived threats of terrorism, gang or drug violence, crimes against children, etc. in certain audiences. Sample question: "How likely do you believe that you will personally be impacted by violence related to terrorism, drug violence, etc.?"
- Develop and tailor messaging that explains, teaches, and promotes the "Going Dark" issue so that common misconceptions are debunked, such as a governmental push for key escrow usage.
- Develop and tailor messaging that advocates for government trust.
- Capitalize on transparency regarding current or ongoing threats in order to foster stronger public understanding.

The aim in employing psychographic targeting is to garner an increase in general trust and support for the government. Furthermore, the government may be able to inform, educate and shape opinion as well as dispel common misconceptions through the utilization of focused targeting to reach individuals who are more likely to oppose or distrust the government based on such misconceived or misinformed beliefs. In addition, directed psychographics could better identify, engage and even recruit the talent required to develop the technologies required to mitigate the going dark problem.

CONCLUSION

The Way Ahead: Policy Recommendations and Next Steps

The going dark problem is projected to persist and challenges on data collection to the US IC and law enforcement grow as technology advances, networks become more global and complex. Going dark is not just an access to data issue, but also encompasses concerns surrounding privacy, technical limitations, legislative shortcomings, and other considerations. Although the IC and law enforcement will never be able to outpace technology, there are some measures they can take to help mitigate potential going dark threats.

Below is a list of potential policy recommendations and next steps for the IC and law enforcement to consider:

1) Broaden the scope of going dark beyond just encryption. Examine other challenges such as authentication in an effort to think outside the box when trying to collect data.

2) Look for data beyond just SIGINT that may contain substantive data. Utilize broader forms of collection, such as human intelligence, and invest more resources on bulk data and metadata collection and tools and capabilities to counter the going dark challenge.

3) Do not be afraid to hack back. While a reactive approach may help minimize damage a proactive approach will thwart potential attacks. Invest in law enforcement technical capabilities and expertise and leverage expertise resident in the public forensic analysis community.

4) Increase public awareness of the challenges faced by law enforcement pertaining to encryption in uncovering national security threat information vital to protecting Americans safety. Engage in public discussion on legal protections and solutions.

5) Increase and enhance partnerships across the intelligence community and law enforcement agencies. There is discrete good work underway that could be accelerated by forging cross-community collaboration and integration across the federal government.

6) Increase public-private sector partnerships. These partnerships could include virtual information-sharing or a fusion cell collocating private sector companies and intelligence or law enforcement to enable better data sharing of critical need-to-know information. Increased interaction will empower the private sector and help build confidence and trust with the government.

7) Establish government liaison officers tasked to manage relations with both the private sector on specific cybersecurity and privacy issues. These officers will build trust and confidence with the private sector and help bridge the gap between the public and private sector on data sharing challenges.

These recommendations are intended to help the Office of the Director of National Intelligence (ODNI) better tackle the going dark problem in not just a reactive, but also a proactive manner. ODNI should draw on experts from the public and private sectors as well as academia to build a collaborative network that can better address going dark challenges. Understanding the intricacies of going dark is not just the responsibility of the government, but of the private sector as well and warrants further study.

REFERENCES

n.d. *Tor Project: Anonymity Online.* https://www.torproject.org/.

Abelson, Hal. 2015. "Keys under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications." *Journal of Cybersecurity, Vol. 1(1).*

Barrett, Brian. 2017. "The Encryption Debate Should End Right Now." *Wired.* 6 30. https://www.wired.com/story/encryption-backdoors-shadow-brokers-vault-7-wannacry/.

Birkland, Thomas A. 1997. "After disaster: agenda setting, public policy, and focusing events." *Georgetown University Press.*

Birkland, Thomas. 1997. *After disaster: agenda setting, public policy, and focusing events.* Washington, DC: Georgetown University Press.

Bowdish, Lawrence. "The Risks of Data Minimization." The Risks of Data Minimization. April 02, 2015. Accessed August 15, 2017. https://www.uschamberfoundation.org/blog/post/risks-data-minimization/42945.

Brenner, Joel, and Rachel Martin. 2014. "Will Obama's NSA Policy Alter The Nature Of Intelligence?,." *NPR.* 1 19. http://www.npr.org/2014/01/19/263921118/will-obamas-nsa-policy-alter-the-nature-of-intelligence.

Byman, Daniel L. 2015. "Comparing Al Qaeda and ISIS: Different goals, different targets." *Brookings.* 4 29. https://www.brookings.edu/testimonies/comparing-al-qaeda-and-isis-different-goals-different-targets/.

Cherny, Michael, and Sagie Dulce. 2017. "Well, That Escalated Quickly! How Abusing Docker Api Led to Remote Code Execution, Same Origin Bypass and Persistence in the Hypervisor via Shadow Containers." *BlackHat.* 7 17. https://www.blackhat.com/us-17/briefings/schedule/index.html#well-that-escalated-quickly-how-abusing-docker-api-led-to-remote-code-execution-same-origin-bypass-and-persistence-in-the-hypervisor-via-shadow-containers-6664.

Chirgwin, Richard. 2017. "Kaspersky fixing serious certificate slip." *The Register.* 1 4. https://www.theregister.co.uk/2017/01/04/kaspersky_fixing_serious_certificate_slip/.

Cimpanu, Catalin. 2017. "Google Outlines SSL Apocalypse for Symantec Certificates." *Bleeping Computer.* 7 29. https://www.bleepingcomputer.com/news/security/google-outlines-ssl-apocalypse-for-symantec-certificates/.

Clapper, James R. 2016. "Worldwide Threat Assessment of the US Intelligence Community." 2 9. https://www.intelligence.senate.gov/sites/default/files/wwt2016.pdf.

Clement, Scott. 2015. "Politics Americans doubt U.S. can stop ‘lone wolf’ attacks, poll finds." *Washington Post.* 12 16. https://www.washingtonpost.com/politics/americans-doubt-us-can-stop-lone-wolf-attacks-poll-finds/2015/12/16/bfcaa102-a3ba-11e5-ad3f-991ce3374e23_story.html?utm_term=.833a63377505.

Comey, James. 2014. "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *FBI.gov.* 10 16. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Comey, James, interview by U.S. Senate Cong. 2015. *Statement before the Committee on the Judiciary Regarding Oversight of the FBI*

Darren Quick, Kim-Kwang Raymond Choo. 2017. "Pervasive social networking forensics: Intelligence and evidence from mobile device extracts." *ScienceDirect.* 5 15. Accessed 2017.

2017. "Demographics of Mobile Device Ownership and Adoption in the United States." *Pew Research Center.* 1 12. Accessed 8 11, 2017. http://www.pewinternet.org/fact-sheet/mobile/.

DiMaggio, Jon. 2016. "Suckfly: Revealing the secret life of your code signing certificates." *Symantec Corporation.* 3 15. https://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates.

Dobbertin, Hans. 1996. "The Status of MD5 After a Recent Attack." *CryptoBytes.* http://webcache.googleusercontent.com/search?q=cache:i5ktD_DKHuMJ:ftp://ftp.arnes.si/packages/crypto-tools/rsa.com/cryptobytes/crypto2n2.pdf.gz+&cd=1&hl=en&ct=clnk&gl=us.

Duncan, Robert. 2013. "US Government aiding spying… against itself." *Netcraft.* 10 16. https://news.netcraft.com/archives/2013/10/16/us-government-aiding-spying-against-itself.html.

Engel, Peyton "Foofus". 2017. "Secret Tools: Learning about Government Surveillance Software You Can't Ever See." *DEF CON.* 7 28. https://www.defcon.org/html/defcon-25/dc-25-speakers.html#Foofus.

2015. "Expired SSL Certificates: How Is This Still a Thing?" *Loom Systems.* 12 10. https://blog.loomsystems.com/2015/12/10/expired-ssl-certificates-how-is-this-still-a-thing/.

Gallagher, Sean. 2015. "What the Government Should've Learned About Backdoors from the Clipper Chip." *Ars Technica.* 12 14. https://arstechnica.com/information-technology/2015/12/what-the-Government-shouldve-learned-about-backdoors-from-the-clipper-chip/.

Gellman, Barton. 2014. "Obama's Restrictions on NSA Surveillance Rely on Narrow Definition of 'Spying'." *The Washington Post.* 1 17. https://www.washingtonpost.com/world/national-security/obamas-restrictions-on-nsa-surveillance-rely-on-narrow-definition-of-spying/2014/01/17/2478cc02-7fcb-11e3-93c1-0e888170b723_story.html?utm_term=.0b740a1bfa24.

Goodin, Dan. 2015. "SHA1 sunset will block millions from encrypted net, Facebook warns." *Ars Technica.* 12 10. https://arstechnica.com/information-technology/2015/12/sha1-sunset-will-block-millions-from-encrypted-net-facebook-warns/.

Greenberg, Andy. 2014. "Hacker Lexicon: What Is End-to-end Encryption?" *Wired.* 11 25. https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

Gregg, Aaron. 2016. "For Some D.C.-Area Companies, Encryption is Big Business." *The Washington Post.* 2 28. https://www.washingtonpost.com/business/on-small-business/for-some-dc-area-companies-encryption-is-big-business/2016/02/27/6af8d056-dcca-11e5-891a-4ed04f4213e8_story.html?utm_term=.8f737f30c592.

Hess, Amy. Statement Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology, Washington DC, April 29, 2015 https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices

"If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine." Harvard Law Review 130, no. 7 (May 9, 2017). May 9, 2017. Accessed August 11, 2017. https://harvardlawreview.org/2017/05/if-these-walls-could-talk-the-smart-home-and-the-fourth-amendment-limits-of-the-third-party-doctrine/.

In re Search Warrant numbers 16-960-M-01 and 16-1061-M to Google, No. 2:16-mj-01061-TJR (United States District Court for the Eastern District of Pennsylvania February 3, 2017).

International Association of Chiefs of Police, Data, Privacy, and Public Safety. 2015. "A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence." 11.

Jeong, Joseph Cox and Sarah. 2016. "FBI Is Pushing Back Against Judge's Order to Reveal Tor Browser Exploit." *Motherboard.* 3 29.

Kerr, Orin. "Supreme Court Agrees to Hear 'Carpenter v. United States,' the Fourth Amendment Historical Cell-Site Case." *The Washington Post*, June 5, 2017. Accessed August 11, 2017. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/05/supreme-court-agrees-to-hear-carpenter-v-united-states-the-fourth-amendment-historical-cell-site-case/?utm_term=.c6337681fe87.

Kassner, Michael. 2015. "Why Government-Mandated Encryption Backdoors are Bad for US Businesses." *TechRepublic.* 7 14. http://www.techrepublic.com/article/why-government-mandated-encryption-backdoors-are-bad-for-us-businesses/.

Knight, Shawn. 2012. "25 PGU Cluster can brute force a Windows password in record time" https://www.techspot.com/news/51044-25-gpu-cluster-can-brute-force-windows-password-in-record-time.html

Maclean, William, and Michael Holden. 2012. ""Lone wolf" gunmen are security puzzle for West." *Reuters.* 3 22. https://www.reuters.com/article/uk-france-detection-idUKBRE82L0V720120322.

Madden, Mary, and Lee Rainie. May 20, 2015. *Americans' Attitudes About Privacy, Security and Surveillance.* Pew Research Center: Internet, Science & Technology.

Maniam, Shiva. n.d. *More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone.* Pew Research Center for the People and the Press.

Martini, Ben, Quang Do, and Kim-Kwang Raymond Choo. n.d. "Mobile Cloud Forensics: An Analysis of Seven Popular Android Apps." *arXiv* . https://arxiv.org/ftp/arxiv/papers/1506/1506.05533.pdf.

Masnick, Mike. 2014. "Good News: Mobile Devices Now Competing To Be Much More Secure Against Prying Eyes." *Techdirt.* 9 19. https://www.techdirt.com/articles/20140918/14030528564/good-news-mobile-devices-now-competing-to-be-much-more-secure-against-prying-eyes.shtml.

Masters, Greg. 2017. "80% of businesses hit by certificate-related outages, study." *SC Media.* 2 2. https://www.scmagazine.com/80-of-businesses-hit-by-certificate-related-outages-study/article/635666/.

Microsoft. n.d. "Digital Signatures and Windows Installer." *Microsoft.* https://msdn.microsoft.com/en-us/library/windows/desktop/aa368289(v=vs.85).aspx.

Microsoft Corporation vs. United States (United States Court of Appeals for the Second Circuit Court July 14, 2016).

Osborne, Charlie. 2017. "Qualys launches CertView security certificate handler for the enterprise." *ZDNet.* 7 24. http://www.zdnet.com/article/qualys-launches-certview-security-certificate-handler-for-the-enterprise/.

Rainie, Lee. September 21, 2016. *The state of privacy in post-Snowden America.* Fact Tank: Pew Research Center.

Rashid, Fahmida Y. "Surveillance is the Business Model of the Internet." Schneier on Security. April 09, 2014. Accessed August 15, 2017. https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html.

Rick Ayers, Sam Brothers, Wayne Jansen. 2014. "Guidelines on Mobile Device." *NIST | National Institute of Standards and Technology.* 5. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.

Sleevi R. 2011. "E-mail message to Chromium." 12 14. https://src.chromium.org/viewvc/chrome?revision=114432&view=revision.

Sabatier, P. A. 1998. "An advocacy coalition framework of policy change and the role of policy-oriented learning therein." *Policy Sciences* (Policy Sciences) 21, 129-168, 142.

Samuel, Alexandra. 2016. "Psychographics Are Just as Important for Marketers as Demographics." *Harvard Business Review.* 3 11. https://hbr.org/2016/03/psychographics-are-just-as-important-for-marketers-as-demographics.

Congressional Research Service. 2017. “Dark Web (CRS Report R44101).”

Sinclair, Nicole. “Former CIA Head: The FBI is Wrong about Apple.” Yahoo Finance. https://finance.yahoo.com/news/former-cia-head--the-fbi-is-wrong-about-apple-165603222.html.

Sumner, Chris. 2017. *Rage Against the Weaponized AI Propaganda Machine.* Las Vegas: The Online Privacy Foundation.

Government Publishing Office. 1986. “Title II - Stored Wire and Electronic Communications and Transactional Records Access.” 121-18 USC 2701-2712.

2016. *Testimony before U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives.* 114th Cong.

2017. "The EU-U.S. Privacy Shield." *European Union.* http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.

Waddell, Kaveh. 2016. "Encryption Is a Luxury." *The Atlantic*. 3 28. https://www.theatlantic.com/technology/archive/2016/03/the-digital-security-divide/475590/.