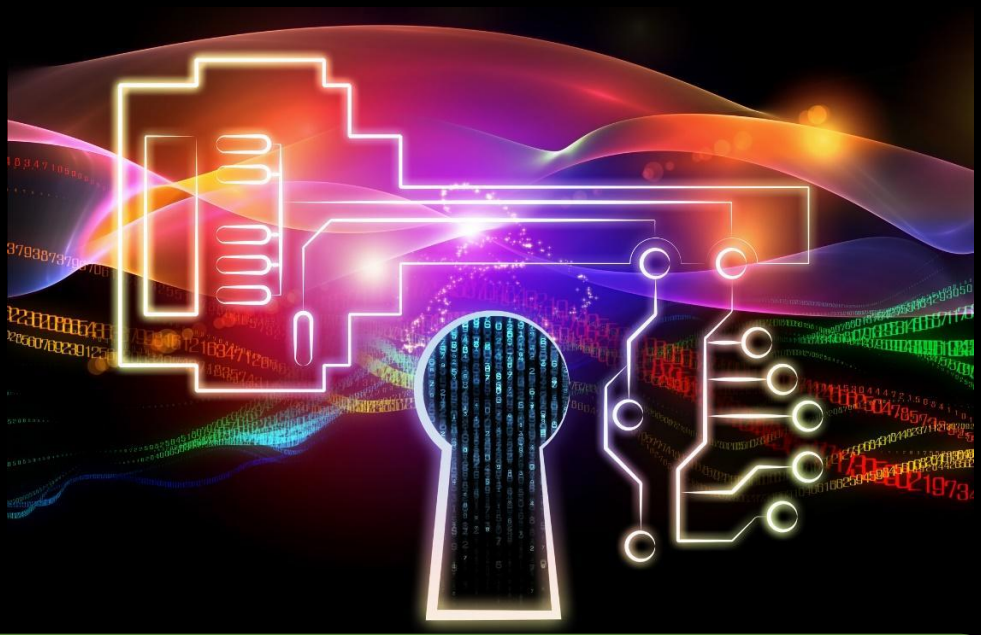

GOING DARKER 2.0: POLICY RECOMMENDATIONS FOR LAW ENFORCEMENT, THE INTELLIGENCE COMMUNITY AND THE PRIVATE SECTOR

Krystle Veda Kaul
Michelle Tucker
G. S. McNamara
Jacqueline Hicks
Colin Bliss
Scott Tosi
Lora Loethen

July 2018

2018 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

ACKNOWLEDGMENTS

We would like to first thank the Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS) for their gracious support throughout the duration of the program.

We could not have completed this study without the unwavering support and dedication of Ms. Lora Loethen, Homeland Programs Manager for the ODNI National Intelligence Manager of Transnational Crime, Homeland and the Western Hemisphere, 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 US, which includes our dedicated Team Lead Krystle Kaul and team members G. S. McNamara, Michelle Tucker, Jacqueline Hicks, Colin Bliss and Scott Tosi.

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 experts from the RSA Conference and the Army Cyber Institute at West Point Academy, government officials and private sector experts. We are grateful for the unique and diverse perspectives, particularly from senior government officials and private sector experts who contributed valuable insight on our study topic.

This collection of policy briefs present 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 and recommendations through extensive qualitative and quantitative research, which included conducting interviews on going dark with subject matter experts within law enforcement, the intelligence community and the private sector. 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 US Government or any commercial entity.

EXECUTIVE SUMMARY

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'[1] through encryption or other means. Strong encryption ensures digital communications are protected for secure commerce and trade to strengthen cybersecurity and to safeguard private information, national security, and the global economy. Unfortunately, rapidly evolving technological advancements—particularly in digital and communications security—impede the ability of US law enforcement and the intelligence community to collect and analyze information that is critical to thwarting potential threats. The recommendations put forth in this paper are intended to help the Office of the Director of National Intelligence (ODNI) tackle the going dark problem and help mitigate potential threats with help from the private sector.

This collection of policy briefs cover the following target areas:

- **Public Awareness about Going Dark**
  - *Employ public surrogates to raise the public's awareness of the challenges imposed by encryption as lawmakers garner support for feasible and balanced mitigation strategies.*
- **Investment in Research Beyond Encryption**
  - *Opportunities exist to mitigate the impact of encryption on intelligence collection through the exploitation of alternate sources and vulnerabilities existing within the expanding plane of open sources and Internet of Things (IoT) "digital exhaust."*[2]
- **Technical Exchanges with Industry**
  - *Technical exchanges with industry reduces capability gaps, better equipping law enforcement to make progress on collecting digital evidence from encrypted devices.*
- **Public Private Partnerships**
  - *Creating liaisons between public and private organizations is an essential element for law enforcement and the intelligence community in solving encryption issues and mitigating potential conflicts between public and private entities.*

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

[2] "Digital exhaust" includes data emitted by various Internet of Things (IoT) technologies (Noyes, 2016). Hereafter, "digital exhaust" will be referred to as digital exhaust.

TABLE OF CONTENTS

PUBLIC AWARENESS ABOUT GOING DARK

Congress should engage with technical and policy experts from industry, academia and government before formally making any policy or legislative decisions. Public perception will play a key role in any publicly disclosed legislative mechanism that is designed to maintain or enhance government surveillance capabilities. The best way to influence public perception is to engage the public through discourse with technical and policy experts.

Executive Summary: The US Government maintains that all levels of law enforcement have the legal authority to intercept and access communications and information pursuant to court orders. However, there is a growing gap between what law enforcement is legally authorized to do and the technical capabilities required to carry out those authorities (Federal Bureau of Investigation, n.d.). The Department of Justice (DOJ), led primarily by the Federal Bureau of Investigation (FBI), has engaged in persistent efforts to raise awareness about this alarming scenario, which is often called the going dark problem. Despite a widespread rigorous awareness campaign, the technologies that exacerbate the problem continue to become more ubiquitous and increasingly prohibit law enforcement's ability to carry out its mission. Congress should engage a variety of stakeholders and subject matter experts so that it can be fully informed about the complexities of the going dark issue and any actions being considered to mitigate the problem. This engagement should occur prior to making any formal policy and legislative decisions.

Scope of Problem: The DOJ has participated in numerous activities over the past eight years to raise public awareness about the challenges facing all levels of law enforcement because of encryption (Savage, September 2010). The FBI has engaged in an aggressive public awareness campaign that has spanned a variety of public and private venues, including Congress, universities, think tanks and others. As the information and communications technologies that underlie going dark have changed and become more omnipresent, the FBI has communicated how the changes are affecting public safety and national security efforts. Despite these sustained attempts, there has been no published measure of the public's awareness on the issue. Furthermore, public perception of the matter may be reflected in consumers' habits such as the purchase and use of devices and applications that are the subject of law enforcement's concerns.

Policy Recommendations: Public perception will play a key role in any publicly disclosed legislative mechanism designed to maintain or enhance government surveillance capabilities. Media coverage will likely cement such a perception. IT companies, media, non-profits and academia follow the going dark issue closely. They are quick to analyze legislative actions leveraging their platforms to inform the public of the repercussions and flaws in legislation. Given the government's long and challenging history with trying to regulate encryption [e.g., the Clipper Chip and Pretty Good Privacy (PGP)], any legislative proposal will be heavily scrutinized, particularly by privacy and information technology security experts (Abelson et al., 2015). The resultant scrutiny will be published in newspapers, websites and blogs which may surface as a hot button issue that could influence electoral preferences (Collins and Patterson, 2016).

The best way to influence public perception regarding proposed legislation is to engage the public via surrogates. These surrogates should consist of technical and policy experts from industry, academia and government. The team's expertise should span a wide range of relevant topics such as communications technology, national security, law enforcement, critical infrastructure, information security, cryptography, constitutional law, policy, economics and commerce. The multifaceted complexities of the going dark problem requires a deep and thorough examination. Rather than trying to mitigate the problem with a one-size-fits all approach, it would be more practical to break it down into manageable components as it is often

the small details that have the most significant consequences. These details are often the most highlighted in the media.

Implementing Policy Recommendations: Getting policy right requires that these experts be engaged early in the process. The intended goals of the policy can be stated, but the stakeholders will have to weigh in on how to achieve the goals. It should be expected in advance that any policy proposals on such a delicate and complex matter will require time to develop and analyze which may be problematic for political reasons, especially given the rapid pace of technological development. Policymakers should familiarize themselves with the research and development processes employed by the academic, science and technology communities. Policymakers should be careful when writing the proposal because any mistakes early on will lead to flawed policies.

In February 2016, Republican Representative Michael McCaul from Texas and Democratic Senator Mark Warner from Virginia introduced a bill with bipartisan support in both the House and Senate titled "The Digital Security Commission Act of 2016" (H.R. 4651 and S.2604, 2016). The purpose of the Act was to establish a commission consisting of a broad array of relevant experts to "assess and make recommendations for policy and practice concerning the issue of multiple security interests in the digital world, including public safety, privacy, national security, and communications and data protection, both now and throughout the next [ten] years." Both bills were referred to as the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations at the end of February 2016. To date, there has not been any formal legislative progress. While this has not caused the going dark debate to cease, it was a formal effort to acknowledge that Congress is a critical stakeholder and should engage with the other stakeholders prior to making policy and legislative decisions.

INVESTMENT IN RESEARCH BEYOND ENCRYPTION

Increasing investment in researching and cultivating alternative routes of intelligence collection and investigative enhancement, during a time of rapidly expanding digital footprints and technology utilization, is critical to combat the going dark problem.

Executive Summary: Law enforcement and the intelligence community can benefit from increased investment, research and development of methods for understanding the intelligence findings and insights that can be derived from a variety of emerging and expanding sources for targeted collections. Focusing solely on the encryption challenge prevents the exploration of other solutions that would potentially offset or mitigate the barrier to collection posed by encryption. A wealth of evolving and increasing amounts of data is available and needs to be analyzed and vetted for the future of intelligence collection at large. The information derived from tertiary sources as part of targeted analysis can assist in counterbalancing the limitations set by encrypted communications and data, aside from providing alternative insights pertinent to investigations and operations.

Identifying and utilizing intelligence collection sources beyond encryption requires additional investment, research and development in order to ensure the lawful exploitation of these emerging sources. This alternative strategic path forward includes a "least bad" approach of exploiting metadata, expanding open source information and using data or digital exhaust from the growing Internet of Things (Hennessey, 2016). Additionally, the future legal implications for employing this strategy should be evaluated simultaneously to prevent potential issues of impeding on one's security and personal privacy.

Scope of Problem: The traditional scope of the going dark problem focuses primarily on encrypted communications and access to information that would require the utilization of decryption technologies, an area in which law enforcement and the intelligence community's technological capabilities and prior methods present both limited and unsustainable long-term strategies. However, other challenges posed to intelligence collection by law enforcement and the intelligence community include the multitude of inaccessible dark web platforms and services, referral-based membership in organizations, steganography[3], and jurisdictions where there is a lack of cooperation and a lack of a uniform expectation of privacy. Like the encryption issue, these trends and technologies have no single solution for offsetting intelligence collection barriers other than looking to innovation and investment for long-term technological solutions.

Policy Recommendations: It is critical to establish internal government and interagency liaison and development teams for conducting future technologies research and development to address alternative collection sources, which will provide long-term solutions to going dark and the barriers set forth by encryption. Future technologies research and development will include quantum computing solutions for decryption as well as expanding the scope of going dark to open source, digital exhaust, IoT or "dark social data"[4] exploitation. The legality of exploring and leveraging the emerging and alternative paths described above is necessary for understanding the available opportunities and for creating the frameworks for future intelligence and investigative use.

There is a need to increase research and development on future open source, social media, "data exhaust"[5] and dark social data exploitation. From a social media standpoint, it is important to understand how platforms evolve, how user bases change dependent on demographics and geography, and how data availability from these platforms may also become limited. Therefore, the future of collection in this space requires a constant refinement of analytical tradecraft as well as technical analytics used on social media platforms, especially in light of the recent Facebook scandal involving Cambridge Analytica. The revelation of Cambridge Analytica's ability to gather massive amounts of personal data from Facebook users triggered Facebook to enforce stricter security and privacy controls. This, in turn, will potentially make future collection more difficult (Granville, 2018). Additionally, it is important to understand the future of data exhaust and IoT emissions as information sources which will work in conjunction with technological shifts towards increasing security both on the Internet and with IoT devices and messaging applications using encryption.

Furthermore, understanding the opportunities presented within data exhaust and IoT emissions as future information sources is vital to the future of intelligence collections considering the going dark problem. Online user activity, behavior and dark social data sharing data provide additional opportunities as a source of intelligence as the amount of available data is expected to grow dramatically (Radium One, 2016). Given the projected increase in data, it will be essential to evaluate the legality of such exploitation of these sources from a research and development standpoint within a future technologies program.

Implementing Policy Recommendations: Creating business cases for investment in the research and development and operationalization of necessary tools and technologies for surpassing collection issues

[3] Steganography is the practice of hiding secret messages in otherwise non-secret mediums (Newman, 2017)

[4] "Dark social data" refers to online social sharing through private channels such as instant messaging and email (Radium One, 2016). Hereafter, "dark social data" will be referred to as dark social data.

[5] "Data exhaust" includes by-products of online user activity (Radium One, 2016). Hereafter, "data exhaust" will be referred to as data exhaust.

posed by encryption is a vital first step. The Criminal Justice Technology Forecasting Group (CJTFG) found that business cases and processes for operationalizing emerging technologies at the federal agency levels are lacking and recommend developing common business cases for technologies that are critical for various agencies (Hollywood, 2018). Additionally, CJTFG proposes that it is imperative to incorporate these business process templates for operationalizing these solutions. In light of the going dark problem, there are multiple sectors within the government, especially the defense and criminal justice departments, which are impacted and could benefit from a common use business case for joint research and development.

Furthermore, it is necessary to have the security, technology and legal knowledge to understand how to properly evaluate and deploy these emerging solutions once a program is established. Identifying and aggregating the right human capital and technical resources will be an additional requirement.

TECHNICAL EXCHANGES WITH INDUSTRY

Technical exchanges with industry can reduce capability gaps, better equipping law enforcement to make progress on collecting digital evidence from encrypted devices.

Executive Summary: Individual law enforcement organizations leverage coalitions to facilitate technical exchanges with industry. Additionally, they receive valuable training on collecting digital evidence from encrypted devices. For instance, authorizing the National Domestic Communications Assistance Center (NDCAC) would support law enforcement organizations with national level outreach to industry in addition to access to valuable training on collecting digital evidence from encrypted devices.

Scope of Problem: The law enforcement community predicts that the "identification, collection, preservation and presentation of digital evidence" will require detailed processes similar to physical evidence (Lazzarini, 2018). However, law enforcement continues to seek information on new software applications, particularly the types of data they collect and how to access encrypted data. The ability of criminals to obfuscate their activities by going dark through encryption or other means hinders US law enforcement organizations from collecting and analyzing information critical to preventing potential threats and solving open investigations (FBI, n.d.). The New York County District Attorney's office assessed the impact of encryption on law enforcement activities and found that while inaccessible devices disrupted ongoing investigations 37.67% of the time, once unlocked the device provided additional evidence 51.14% of the time (DOJ, Appendix F, 2018). Law enforcement organizations across the nation are actively collaborating to identify and reduce gaps in their ability to collect encrypted digital evidence, but there is a need for a focused effort to address national level issues (DOJ, 2018). In December 2016, the bipartisan Encryption Working Group with members from the House Judiciary Committee and the House Energy and Commerce Committee released its year-end report declaring a call to action, "Congress should foster cooperation between the law enforcement community and technology companies" (House Judiciary Committee and House Energy and Commerce Committee Encryption Working Group 2016, 7). However, this recommendation was never implemented which is why individual law enforcement organizations must continue to develop their own relationships.

Policy Recommendations: Lawmakers can support law enforcement organizations by funding institutions that facilitate technical exchanges on critical national security issues. Law enforcement organizations are actively building relationships with industry to keep up with ever-changing vendor specific privacy policies and security features (Thompson, 2018). Several organizations such as The National Computer Forensics

Institute, The Law Enforcement Cyber Center, and the National Domestic Communications Assistance Center (NDCAC) provide law enforcement organizations with formal means of establishing and maintaining relationships with industry for the purposes of technical exchange (Law Enforcement Cyber Center, n.d.). Many organizations also offer training to ensure law enforcement personnel understand the data available within software applications and methods of access. Increased collaboration with industry will help law enforcement communities better understand their options when seeking access to locked devices that may contain evidence pertinent to an ongoing investigation.

Implementing Policy Recommendations: The Encryption Working Group recommends authorizing and modernizing the NDCAC which has a budget of $10.9M which falls under the DOJ (DOJ, 2018). The NDCAC does not play a role in investigations, but it is a resource for exchanging technical knowledge (House Judiciary Committee and House Energy and Commerce Committee Encryption Working Group 2016, 9). Additionally, the current budget funds an Industry Relations Program with the goal of developing and maintaining relationships with industry to exchange information on issues that rise to a national level ensuring law enforcement's understanding of new services and technologies through information sharing and coordination assistance (DOJ, 2017). The NDCAC has a broad outreach program for law enforcement and industry which could be expanded (DOJ, 2018). The center has trained over 7,200 law enforcement personnel and there are plans to expand the breadth and depth of trainings offered (DOJ, 2018). In particular, there is a program specialized in handling mobile device evidence which is developed in a train-the-trainer format to increase its impact nationwide (DOJ, 2018).

According to the Director of the NDCAC, "the Authorization has not happened yet. There are several associations that have been asking that the NDCAC be authorized as well" (NDCAC Director, e-mail, 2018). Authorizing and modernizing the NDCAC would stabilize the budget which has been in decline over the past six years (DOJ, Appendix D, 2018). The promising and comprehensive NDCAC strategic plan seeks to leverage working groups to strengthen partnerships and leverage technology to improve capability and capacity (DOJ, Appendix D, 2018).

PUBLIC PRIVATE PARTNERSHIPS

Creating liaisons between public and private organizations is an essential element for law enforcement and the intelligence community in solving encryption issues and mitigating potential conflicts between public and private entities.

Executive Summary: By nature, the going dark problem requires cooperation between public and private entities to permit law enforcement and government to lawfully access data while protecting private companies' customer data and intellectual property. The 2015-2016 Apple and FBI debate over decryption highlighted the negative blowback associated with attempting to force private companies to decrypt data. Rather than assume an authoritative and confrontational role, government agencies should seek a cooperative and mutually beneficial relationship to reach compromise and satisfy both parties' goals. Just having a liaison without a full public private partnership, will only yield short-term results instead of lasting solutions. Liaisons between public and private entities are currently decentralized in agency, geographic location and messaging. Therefore, law enforcement and the intelligence community should centralize liaisons through the creation of public private partnerships (PPPs) as a forcing mechanism to consolidate efforts, reach a broad audience, centralize messaging and de-conflict issues prior to situations arising.

Scope of Problem: While the use of liaison personnel between agencies and departments within federal and state governments has increased in recent decades as a major component to the whole-of-government approach, much less has been done to bridge the gap between public and private entities. This is largely due in part to the high cost to the government of embedding liaison personnel in individual private companies in comparison with the relative low cost of placing personnel in partner agencies and departments. Additionally, private companies that do not rely heavily on government contracts are generally wary of a permanent government employee presence.

A current issue at the government agency and department level of government is the decentralized nature of liaisons with public partners. For example, the FBI, primarily acts as the liaison at the field office level, with little coordination conducted at higher echelons. Other government agencies similarly liaise based on geographical divisions which create situations in which multiple personnel from the same public entity liaise with the same private entity. The systemic issues created by this framework are two-fold: First, agencies are wasting countless hours conducting redundant liaison with the same public companies across different geographical areas of responsibility; and Second, agencies and departments lack consistent messaging which convey conflicting information from other adjacent liaison elements.

A second major issue for public private liaisons is the overwhelming number of private entities that require direct liaisons from government agencies. Just liaising with individual companies without a partnership is both inefficient and costly to law enforcement and the intelligence community. Therefore, it is more effective and efficient to use a more centralized means of liaising through a partnership to reach more private sector organizations.

Policy Recommendations: In place of the current decentralized approach to public private liaisons, federal law enforcement and the intelligence community should establish Public Private Partnerships (PPPs) to address the going dark problem.

Implementing Policy Recommendations: Establishing centralized Public Private Partnerships consisting of multi-agency government elements and public corporations and companies will alleviate much of the redundancy and cost inefficiencies currently experienced in conducting liaison work. Though task-oriented PPPs currently exist, such as the National Cyber Security Alliance, they typically exist between one government agency or department and multiple public companies (Busch, 2012). However, the going dark issue affects law enforcement, intelligence collection, and military action which directly impacts all facets of the intelligence community. However, in order for any PPP to survive private sector members must be offered economic incentives to join a PPP or else the organization will risk failure (Carnegie Mellon University, 2010).

Establishing PPPs between single agencies or departments is both inefficient and counterproductive as private sector participants would be forced to be members in multiple PPPs. Rather, a single PPP involving all agencies and departments within the intelligence community would be required in order to ensure consistent messaging, demands and coordination within the public sector.

Additionally, the government can utilize the seventy-eight existing Department of Homeland Security Fusion Centers by expanding their role to act as a medium for communication between state and local law enforcement and PPPs. Additionally, federal interagency bodies and commissions can also serve as an additional component to public private liaisons as bolstered support (DHS, 2017). In turn, this will allow new information and best practices to flow down from federal law enforcement and the intelligence community to state and local law enforcement. Additionally, growing encryption concerns will flow up to the federal level and be addressed in a centralized platform through Public Private Partnerships. Such

partnerships will create a unique platform for public private partnerships which will help build trust and address the going dark problem paving the way for a new future.

REFERENCES

Abelson, Harold, Anderson, Ross and Bellovin, Steven M. et al. July 6, 2015. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." *Computer Science and Artificial Intelligence Laboratory*. 1-3. http://hdl.handle.net/1721.1/97690.

Busch, Nathan E. and Givens, Austen D. October 2012. "Public-Private Partnerships in Homeland Security: Opportunities and Challenges." *Homeland Security Affairs 8*. Article 18. Accessed June 10, 2018. https://www.hsaj.org/articles/233.

Collins, Terry and Patterson, Dan. September 26, 2016. "Where Clinton, Trump Stand on Seven Big Tech Issues." *CNET*. Accessed June 26, 2018. https://www.cnet.com/news/clinton-trump-7-tech-issues-encryption-cybersecurity-apple/.

Department of Homeland Security. 2017. "2016 National Network of Fusion Centers Final Report." Accessed June 10, 2018. https://www.dhs.gov/sites/default/files/publications/2016_National _Network of_Fusion_Centers_Final_Report.pdf.

Federal Bureau of Investigation. n.d. "Going Dark." Accessed June 11, 2018. https://www.fbi.gov/services/operational-technology/going-dark.

Granville, Kevin. March 18, 2018. "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens." *New York Times*. https://www.nytimes.com/2018/03/19/technology/ facebook-cambridge-analytica-explained.html.

Hennessey, Susan. 2016. "Lawful Hacking and the Case for a Strategic Approach to 'Going Dark'." 2016. Brookings Institution. https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/.

Hollywood, John S., Woods, Dulani and Lauland, Andrew et al. 2018. "Addressing Emerging Trends to Support the Future of Criminal Justice: Findings of the Criminal Justice Technology Forecasting Group." Santa Monica, CA: *RAND Corporation*. https://www.rand.org/pubs/research _reports/RR1987.html.

House Judiciary Committee and House Energy and Commerce Committee Encryption Working Group. 2017. "Encryption Working Group Year-End Report." December 20, 2017. Accessed June 8, 2018. https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf.

Law Enforcement Cyber Center. n.d. "About." Accessed June 18, 2018. http://www.iacpcybercenter.org/.

Lazzarini, Michael. 2018. "Death by Wi-Fi: How Computer Technology Will Impact Violent Crime Investigations." Accessed June 18, 2018. http://lawofficer.com/investigations/death-wifi/amp/?__twitter_impression=true.

National Domestic Communication Assistance Center, Department of Justice. 2017. "Executive Advisory Board Meeting Minutes November 2017." Accessed June 18, 2018. https://ndcac.fbi.gov/file-repository/november-2017-eab-minutes.pdf/view.

National Domestic Communication Assistance Center, Department of Justice. April 11, 2018. "April 2018 Executive Advisory Board Meeting Minutes Appendices—'Encryption and the Impact on Law Enforcement'." Appendix F. New York County District Attorney's Office Presentation to NDCAC Executive Advisory Board. Accessed June 18, 2018. https://ndcac.fbi.gov/file-repository/april-2018-eab-meeting-appendices.pdf/view.

National Domestic Communication Assistance Center, Department of Justice. April 11, 2018. "Executive Advisory Board Meeting Minutes April 2018." https://ndcac.fbi.gov/file-repository/april-2018-eab-minutes-20180608.pdf/view.

National Domestic Communication Assistance Center, Department of Justice. 2018 "Executive Advisory Board Meeting Minutes, April 2018, Appendix D, Mission Statement and Strategic Objectives." https://ndcac.fbi.gov/file-repository/april-2018-eab-meeting-appendices.pdf/view.

Newman, Lily. June 2017. "Jacker Lexicon: What is Stenography?" Security, *Wired*. Accessed 10 June 2018. https://www.wired.com/story/steganography-hacker-lexicon/.

Noyes, Katherine. "5 Things You Need to Know about Data Exhaust." May 13, 2016. *PCWorld*. Accessed June 02, 2018. https://www.pcworld.com/article/3069507/5-things-you-need-to-know-about-data-exhaust.html.

Radium One. June 7, 2016. "The Dark Side of Mobile Sharing." https://radiumone.com/wp-content/uploads/2016/08/radiumone-the-dark-side-of-mobile-sharing-June-7-2016.pdf.

Savage, Charlie. September 27, 2010. "U.S. Tries to Make It Easier to Wiretap the Internet." *New York Times*. Accessed 13 June 2018. https://www.nytimes.com/2010/09/27/us/27wiretap.html.

Software Engineering Institute Carnegie Mellon University. 2010. "Public-Private Partnerships: Essential for National Cyber Security." *Cert's Podcasts: Security For Business Leaders*. Accessed June 15, 2018. https://resources.sei.cmu.edu/asset_files/Podcast/2010_016_102_67854.pdf.

Thompson, Troy. March 6, 2018. "Grayshift Will Allegedly Unlock 300 iPhone X Devices for $15,000." Accessed June 8, 2018. https://www.idropnews.com/news/graykey-will-allegedly-unlock-300-iphone-x-devices-15000/65115/.