NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE KEY TO LAWFUL ACCESS: AN ANALYSIS OF THE ALTERNATIVES OFFERED IN THE ENCRYPTION DEBATE

by

William R. Mack

September 2020

Co-Advisors:	Lynda A. Peters (contractor) Shannon A. Brown

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2020	**3. REPORT TYPE AND DATES COVERED** Master’s thesis

4. TITLE AND SUBTITLE THE KEY TO LAWFUL ACCESS: AN ANALYSIS OF THE ALTERNATIVES OFFERED IN THE ENCRYPTION DEBATE	**5. FUNDING NUMBERS**
6. AUTHOR(S) William R. Mack	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis examines the lawful access challenge that law enforcement and intelligence agencies face when seeking to obtain communications and mobile electronic devices that cannot be penetrated and that include strong encryption protocols. This encrypted data is inaccessible despite government agencies holding court-approved search warrants and wiretap orders authorizing access. Technology companies, cryptographers, and privacy advocates have argued for years that allowing such lawful access for government agencies will leave Americans’ personal information vulnerable to cyber criminals and nation-state adversaries. These groups have offered alternatives to lawful access, which they argue can stand in lieu of the lawful access government agencies argue should be mandated. This thesis uses a policy options analysis to evaluate the viability of these alternatives to mandated lawful access. This thesis explores law enforcement and intelligence agencies’ need for access to encrypted data through a review of incidents in which access proved fruitful and incidents in which lack of access was detrimental to public safety, homeland and national security, criminal investigations, etc. This thesis finds that the alternatives offered in place of lawful access are not adequate in ensuring government agencies are able to fulfill their law enforcement and intelligence missions.

14. SUBJECT TERMS encryption, end-to-end, going dark, lawful hacking, lawful access	**15. NUMBER OF PAGES** 131
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

THE KEY TO LAWFUL ACCESS: AN ANALYSIS OF THE ALTERNATIVES OFFERED IN THE ENCRYPTION DEBATE

William R. Mack
Resident Agent in Charge, U.S. Secret Service, Department of Homeland Security
BA, Rutgers University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2020**

Approved by: Lynda A. Peters
Co-Advisor

Shannon A. Brown
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines the lawful access challenge that law enforcement and intelligence agencies face when seeking to obtain communications and mobile electronic devices that cannot be penetrated and that include strong encryption protocols. This encrypted data is inaccessible despite government agencies holding court-approved search warrants and wiretap orders authorizing access. Technology companies, cryptographers, and privacy advocates have argued for years that allowing such lawful access for government agencies will leave Americans' personal information vulnerable to cyber criminals and nation-state adversaries. These groups have offered alternatives to lawful access, which they argue can stand in lieu of the lawful access government agencies argue should be mandated. This thesis uses a policy options analysis to evaluate the viability of these alternatives to mandated lawful access. This thesis explores law enforcement and intelligence agencies' need for access to encrypted data through a review of incidents in which access proved fruitful and incidents in which lack of access was detrimental to public safety, homeland and national security, criminal investigations, etc. This thesis finds that the alternatives offered in place of lawful access are not adequate in ensuring government agencies are able to fulfill their law enforcement and intelligence missions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
AQAP	Al Qaeda in the Arabian Peninsula
CALEA	Communications Assistance for Law Enforcement Act
CESA	Cyberspace Electronic Security Act
CIA	Central Intelligence Agency
CPS	Crown Prosecution Service
DA	district attorney
DOJ	Department of Justice
EARN IT	Eliminating Abusive and Rampant Neglect of Interactive Technologies
EFF	Electronic Frontier Foundation
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
GCHQ	Government Communications Headquarters
GRU	Main Intelligence Directorate
IaaS	Infrastructure as a Service
IC	U.S. Intelligence Community
IG	Inspector General
ISIL	Islamic State of Iraq and the Levant
ISIS	Islamic State of Iraq and Syria
NCMEC	National Center for Missing & Exploited Children
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PaaS	Platform as a Service
SaaS	Software as a Service
TATP	triacetone triperoxide

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis examines the encryption debate in which law enforcement and the U.S. Intelligence Community (IC) face a lawful access challenge, smartphones and messaging applications inaccessible because of encryption, even when court-issued search warrants and wiretap orders have been approved by a judge.[1] Computer scientists, cryptographers, technology companies, and privacy advocates have all written extensively on the need for strong encryption while warning that any mandate that allows for lawful access by the government leaves important data vulnerable to exploitation by adversaries, criminals, and corrupt officials. Many have proposed alternative options for law enforcement and the IC on which to rely. These alternatives are analyzed in this paper for their viability as policy options in place of mandated lawful access.

Government agencies have sounded an alarm for years that terrorists, child pornographers, and other criminals are benefitting from encryption. The San Bernardino attacks in 2015, where a married couple shot and killed 11 people, brought the encryption debate into the spotlight.[2] Only two years prior, the Snowden disclosures sparked mass surveillance concerns causing a breach of the public's trust in corporations and the government to protect Americans' personal information. The result has been default encryption as a de facto commercial standard; impenetrable security protocols are incorporated into applications and devices, designed to keep all, even the developers and manufacturers, from being able to access encrypted data.

End-to-end encryption makes data passed between users of mobile messaging applications unreadable by anyone intercepting it, including the application makers. Law enforcement thus cannot access these communications despite having a wiretap order. Statistics compiled by the Administrative Office of the United States Courts indicates that

[1] "The Lawful Access Challenge," Federal Bureau of Investigation, accessed August 6, 2020, https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch/lawful-access.

[2] Zusha Elinson and Dan Frosch, "San Bernardino Shooting: How the Carnage Unfolded; Witnesses Recount Horror, Suspense as Bursts of Gunfire Interrupted Office Party," *Wall Street Journal*, December 4, 2015, sec. U.S.

law enforcement encounters with encrypted data in motion that could not be deciphered more than doubled between 2018 and 2019.[3]

In addition, law enforcement is encountering data at rest on mobile devices, like an iPhone used by one of the San Bernardino shooters, which is also inaccessible. This issue affects all levels of law enforcement including local, state, and federal agencies. Devices that may hold a plethora of important evidence like contact lists, photos, and journals are impenetrable because device and operating systems feature default settings that only decrypt a device's data when the correct passcode is entered. This feature leaves evidence unrecoverable and intelligence uncollected.

Law enforcement identified this issue long before San Bernardino, while encryption was much less widespread. Various solutions were proposed, including a device called the Clipper Chip that would have given law enforcement the ability to intercept and read encrypted communications. Privacy advocates vocally opposed this capability, sparking the "Crypto Wars" of the 1990s.[4] This chip was eventually found to be defective but it laid the foundation for today's ongoing debate.[5] Now, law enforcement calls for lawful access without offering a specific technical solution itself, preferring to consign that to the individual technology companies, each with their own platforms.[6] The most relevant legislation related to the encryption debate is the Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications carriers be able to decrypt or facilitate the decryption of data that has been encrypted by a carrier's customers unless

[3] "Wiretap Report 2018," Administrative Office of the United States Courts, last updated December 31, 2018, http://www.uscourts.gov/statistics-reports/wiretap-report-2018; "Wiretap Report 2019," Administrative Office of the United States Courts, last updated December 31, 2019, http://www.uscourts.gov/statistics-reports/wiretap-report-2019.

[4] Richard A. Spinello, *Cyberethics: Morality and Law in Cyberspace*, 6th ed. (Burlington, MA: Jones & Bartlett Learning, 2017), 219–21.

[5] Kristin M. Finklea, *Encryption and the 'Going Dark' Debate*, CRS Report No. R44481 (Washington, DC: Congressional Research Service, 2017), 14, https://crsreports.congress.gov/product/details?prodcode=R44481.

[6] Christopher Wray, "Finding a Way Forward on Lawful Access," Federal Bureau of Investigation, October 4, 2019, https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access.

the carrier encrypted the data and can thus decrypt it itself.[7] CALEA ensures that law enforcement agencies can intercept communications in an evolving technological environment, but the Act does not apply to many of the types of companies today that provide messaging applications that use end-to-end encryption.[8] Congress expanded CALEA in 2004 to include some internet communications services, but not the applications using end-to-end encryption that have become popular in recent years.[9] No legislation currently addresses lawful access for encrypted smartphones.

The literature on the encryption debate often asserts that the government should seek other options for obtaining the information it needs instead of mandating lawful access. Lawful hacking is one such option, when law enforcement and intelligence agencies exploit vulnerabilities to defeat encryption and access data in a readable format. Literature on the subject argues that lawful hacking is an adequate balance between the two sides of the encryption debate. However, when analyzed in the context of case studies of counterterrorism and criminal investigation, it falls short because of its unreliability in accessing data and its infeasibility in implementing the method across U.S. police agencies.

Other alternatives also fall short. Metadata, or data about data, also fails to replace lawful access adequately since it does not reveal the important content of communications, specifically, valuable evidence in criminal investigations and actionable intelligence in counterterrorism pursuits. Compelling users to disclose passcodes of devices permitting access is unusable in instances where users are not present to unlock a device. In addition, the courts have not settled on the implications for civil rights. Accessing backup data in the cloud is also inadequate as it is easily avoided by nefarious actors and must often be affirmatively engaged to back up devices fully. While all these alternatives are in use today

[7] James A. Lewis, Denise E. Zheng, and William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (Washington, DC: Center for Strategic and International Studies, 2017), 36, https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data; *Legal Information Institute*, "Title 47 U.S. Code § 1002—Assistance Capability Requirements."

[8] Lewis, Zheng, and Carter, 36.

[9] "OMB Approves CALEA Compliance Monitoring Report for Providers of Facilities-Based Broadband Internet Access and Interconnected VOIP Service; Reports Are Due February 12, 2007," Federal Communications Commission, December 14, 2006, https://www.fcc.gov/document/omb-approves-calea-compliance-monitoring-report-providers-facilities.

by law enforcement, they do not meet the needs of public safety and homeland security agencies, even if viewed in unison.

This thesis analyzes these alternatives using several case studies to illustrate both the importance of accessing often-encrypted data, and the frustrations that come when important evidence cannot be accessed. These case studies include an Islamic State of Iraq and Syria (ISIS) recruiter who used an encrypted messaging application to communicate with plotters, a subject that received child pornography via the internet, and a member of the Saudi Arabian military who attacked sailors at a Florida naval base and whose phone was encrypted. The case studies presented in this thesis aid in analyzing the viability of alternatives to lawful access.

This thesis finds that the need for lawful access for law enforcement and intelligence agencies is legitimate. Alternatives presented by experts involved in the debate on encryption are unable to meet that need. Without further action, this debate will continue and law enforcement and intelligence agencies will continue to be frustrated by encryption.

ACKNOWLEDGMENTS

I would like to thank my wife and children first and foremost. Without their love and support, this endeavor would not have been possible.

I also offer my gratitude to my advisors, Dr. Shannon Brown and Lynda Peters, whose support and guidance was vital to this final product.

I would also like to thank my colleagues at the United States Secret Service, especially those in the Dallas Field Office and the Office of Intergovernmental and Legislative Affairs who supported my application and nomination, as well as friends and former colleagues at the Department of Homeland Security Office of Operations Coordination for their support and encouragement. Particular thanks go to the members of the Tyler Resident Office, all of whom often took on additional responsibilities in my absences while participating in this program.

Finally, I wish to thank my colleagues in Cohort 1901/1902 who have opened my eyes even wider to the diversity of the homeland security effort.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

On December 2, 2015, Syed Rizwan Farook and his wife, Tashfeen Malik, entered the Inland Regional Center in San Bernardino, CA, during an office party for the San Bernardino County Public Health Office.[1] They were wearing body armor and carrying assault rifles. The couple opened fire on the party, killing 14 and injuring another 21 people. The two fled but police located them a few hours later, engaged them in a shootout, and killed them. Investigators would later find Farook's iPhone that had been issued to him by the Public Health Office sitting in a black Lexus sedan owned by Farook's mother. The Federal Bureau of Investigation (FBI) could not access any data on the phone due to its encryption setting. This phone became the center of the debate on encryption and law enforcement's ability, or lack thereof, to access encrypted devices like Farook's iPhone. A court battle ensued between the Department of Justice (DOJ) and Apple, Inc., in which the government requested that Apple grant access to the encrypted device but Apple refused, calling the FBI request dangerous.[2] As the case unfolded, the FBI eventually gained access to the phone when a third party stepped in to help. Shortly afterward, the DOJ withdrew its petition in court, so no legal decision was rendered regarding law enforcement access to an encrypted device. This tragic incident reveals the challenge encryption poses to the effectiveness of law enforcement agencies' work.

Approximately a year before the attack in San Bernardino, in September 2014, the technology companies Google and Apple—that produce mobile devices and software—introduced default encryption on products sold to the public. As such, strong encryption has become the standard, and law enforcement is often unable to search devices despite

[1] Zusha Elinson and Dan Frosch, "San Bernardino Shooting: How the Carnage Unfolded: Witnesses Recount Horror, Suspense as Bursts of Gunfire Interrupted Office Party," *Wall Street Journal*, December 4, 2015, sec. US.

[2] Tim Cook, "Customer Letter," Apple, Inc., February 16, 2016, http://www.apple.com/customer-letter/.

court approval because employing encryption on these devices locks out law enforcement in addition to everyone else.[3]

In October 2014, former FBI Director James Comey exposed the serious challenges that encryption would pose to public safety and national security in the future.[4] In explaining the significance, Comey described a sex offender convicted in 2014 of murder after that sex offender lured a 12-year-old boy out of his house, and then killed him.[5] Evidence recovered from both the killer's phone and the victim's phone was vital to securing a conviction.[6] Comey also detailed how law enforcement was facing situations where it could not access needed information because of encrypted messaging applications.[7] In 2010, the Director of the Administrative Office of the U.S. Courts reported that of the six state or federal court ordered wiretaps involving encryption, all were deciphered.[8] In 2018, the same body reported that 220 wiretaps encountered encryption with 192 of them unable to be deciphered.[9] The following year, 2019, the numbers surged with 464 wiretaps encountering encryption with 438 unable to be read.[10] These numbers do not even account for the likely much higher number of orders never sought since law enforcement is fully aware of what it cannot access.[11] Without access to

[3] Joe Miller, "Google and Apple Encrypt by Default," BBC News, September 19, 2014, https://www.bbc.com/news/technology-29276955.

[4] James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," Federal Bureau of Investigation, October 16, 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[5] Comey.

[6] Comey.

[7] Comey.

[8] Administrative Office of the United States Courts, *Wiretap Report 2010* (Washington, DC: Administrative Office of the United States Courts, 2011), 9, https://www.uscourts.gov/statistics-reports/wiretap-report-2010.

[9] "Wiretap Report 2018," Administrative Office of the United States Courts, last updated December 31, 2018, http://www.uscourts.gov/statistics-reports/wiretap-report-2018.

[10] "Wiretap Report 2019," Administrative Office of the United States Courts, last updated December 31, 2019, http://www.uscourts.gov/statistics-reports/wiretap-report-2019.

[11] James A. Lewis, Denise E. Zheng, and William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (Washington, DC: Center for Strategic and International Studies, 2017), 13, https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data

such data, law enforcement risks lacking the evidence necessary to secure convictions and enforce the law.

Since the San Bernardino attack, government agencies in the United States have continued to raise the issue of the need for lawful access to make it possible for the government to receive decrypted data.[12] However, Congress has neither been convinced of the need to create legislation requiring lawful access nor have companies like Apple and Google changed their stance on encryption.

The encryption debate has featured a wide range of terminology throughout the years, often with nuanced differences as the language has evolved. A summary of the various terms is included as follows, and each is explored further in the Literature Review section.

- Scholars and technology experts often refer to law enforcement's goal as *exceptional access* based on the concept of access created specifically for the government.[13]

- The FBI has previously referred to the issue as *going dark*, which suggests that criminal and terrorist use of encryption makes it difficult to track the perpetrators.[14]

- Law enforcement has favored the use of the phrase *lawful access challenge* to describe the issue faced with encryption and the government's preference for requiring telecommunications companies to

[12] Kate Fazzini, "FBI Director Wray: I Strongly Share Barr's Concerns about Encrypted Devices and Messaging Platforms, Cites Sutherland Springs Apple Case," CNBC, July 25, 2019, https://www.cnbc.com/2019/07/25/fbi-director-wray-i-strongly-share-barrs-concerns-about-encryption.html; Lauren Feiner, "AG Barr Says Tech Companies Need to Make Encrypted Messages Accessible to Law Enforcement," CNBC, July 23, 2019, https://www.cnbc.com/2019/07/23/bill-barr-tells-tech-to-open-encrypted-messages-for-investigations.html.

[13] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers* (Washington, DC: The National Academies Press, 2018), 1–3, 9, https://doi.org/10.17226/25010.

[14] "Going Dark," Federal Bureau of Investigation, March 5, 2020, https://web.archive.org/web/20200305041805/https://www.fbi.gov/services/operational-technology/going-dark.

> be required to produce decrypted data after being presented with legal process like a search warrant or wiretap order.[15]

This thesis uses the term lawful access challenge when referring to the issue that law enforcement faces with encryption. Since the literature often refers to the access that the government seeks as exceptional access, this thesis uses that phrase in the context of discussions about the literature.

While law enforcement is making the case for lawful access, a host of privacy advocates, technology companies, and cryptographic experts have been explaining why such access is either dangerous or unnecessary. Often, their arguments propose alternatives to lawful access. In 2013, for example, numerous computer scientists and scholars collaborated on a paper that argued that new technologies would increasingly provide the information law enforcement needs without the need to access encrypted data.[16] Scholars have also cited "lawful hacking," which would authorize law enforcement to hack into encrypted systems, as an option for dealing with encryption.[17] Though computer scientists and cryptographers have offered alternatives to accessing encrypted data, these alternatives have received little scrutiny as to their viability as law enforcement policy.

Since the San Bernardino shooting, encryption has been widely discussed. Scientists have written about the need to maintain strong encryption and the dangerousness of lawful access. Law enforcement has spoken out about the risk encryption poses to public safety and criminal justice. This thesis aspires to determine whether the government needs to gain lawful access to encrypted data and whether the alternatives proposed are viable replacements for agencies to use in lieu of a lawful access mandate.

[15] "The Lawful Access Challenge," Federal Bureau of Investigation, accessed August 6, 2020, https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch/lawful-access.

[16] Urs Gasser et al., *Don't Panic: Making Progress on the 'Going Dark' Debate* (Cambridge, MA: Berkman Center for Internet & Society at Harvard Law School, 2016), 2–3, https://dash.harvard.edu/bitstream/handle/1/28552576/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf?sequence=1&isAllowed=y.

[17] Steven M. Bellovin et al., "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property* 12, no. 1 (2014): 5, https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip.

B. RESEARCH QUESTIONS

What is the justification for mandating lawful access for law enforcement and the U.S. Intelligence Community (IC) to encrypted devices and messaging applications? To what degree are the alternatives suggested by cryptographers, privacy experts, and other scholars effective policy options for the government in place of legislative or policy initiatives that would ensure law enforcement and the IC access to encrypted data?

C. LITERATURE REVIEW

Many scholars narrowly frame the issue of encryption as a debate between U.S. law enforcement, primarily the FBI, and privacy experts. Yet, a wide range of stakeholders has an interest in this debate, including the following: local, state, and federal law enforcement, mobile device manufacturers, messaging application companies, cryptographers, computer scientists, and privacy experts. Some of these stakeholders have produced important papers, articles, and reports on the issue that have addressed topics like law enforcement access, maintaining strong encryption, and implementing alternatives to decryption. An abundance of opinion articles, blog posts, and websites discuss these issues as well. In addition, many well-respected, experienced, and knowledgeable professionals have weighed in on the encryption debate over the past several years and have provided some significant insight into a myriad of aspects about it. This literature review addresses the following main schools of thought in turn: maintaining strong encryption, seeking alternatives to search warrants and wiretaps, and allowing access for law enforcement.

1. Maintaining Strong Encryption

Many experts in the fields of cryptography and computer science have waded into the encryption debate by explaining why the policy in the United States should favor strong encryption with no allowance for lawful access. One notable thing about many of the works that these experts have written is the collaboration between academics and experts in the field. One such work, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," was co-authored by 15 experts, many of whom are well-known and well-respected names on the subject like Susan

Landau, Bruce Schneier, and Matt Blaze.[18] Another important work that supports strong encryption has 11 experts in various arenas as authors.[19] Continuing with this trend is another oft-cited, pro-encryption work authored by 12 "signatories" who include academics and former government officials Susan Landau, Jonathan Zittrain and Bruce Schneier.[20] This trend of large numbers of co-authors, many of whom are the foremost experts in their fields, is likely a testament to how concerned many are about the potential effects of allowing the government to have access to encrypted devices. As Gasser et al. state, "we believe that law enforcement has failed to account for the risks inherent in exceptional access systems."[21]

Among all the literature that focuses upon maintaining the status quo of strong encryption, many authors argue that granting law enforcement access to encrypted data compromises the security of that data, which in turn, makes encrypted products susceptible to attack and exploitation by online criminals. Schneier argues that encryption is important in safeguarding users from online criminals and eavesdropping governments.[22] Allowing law enforcement access to encrypted systems would amplify these risks.[23] "Keys under Doormats" argues that exceptional access is antithetical to the methods used today to secure the internet because the methods use temporary keys for decryption and authentication rather than permanent keys vulnerable to theft or exploitation.[24] Thus, these scholars favor a policy of permitting no restrictions or special allowances for any government agencies regardless of need or legal process.

[18] Harold Abelson et al., "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1, no. 1 (July 7, 2015): 69–79, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[19] Lillian Ablon et al., *Going Dark: Implications of an Encrypted World* (New York: New York Center for Advanced Study in Terrorism at Colombia University, 2017), iv–v, https://nsiteam.com/going-dark-implications-of-an-encrypted-world/.

[20] Gasser et al., *Don't Panic*, Signatories.

[21] Abelson et al., "Keys under Doormats," 1.

[22] Gasser et al., *Don't Panic*, Appendix A.

[23] Gasser et al., Appendix A.

[24] Abelson et al., "Keys under Doormats," 12.

Another common theme in the literature favoring strong encryption is that the pursuit of mandated access is technologically impossible or at least extremely difficult. Scientists have written about the technical issues surrounding access for law enforcement for many years. In 1997, 11 scientists wrote that a proposal for law enforcement access to encrypted data would likely result in the development of unintended vulnerabilities and cited an NSA key escrow system found to have multiple "failures" over the four years since it had been designed.[25] A report by Lillian Ablon et al. discusses not only current technical issues but also examines likely future problems.[26] In it, 11 scholars argue that the future will lead to ever-increasing amounts of encrypted data that will overwhelm and overcome computers used to crack encryption keys.[27] Clearly, a large number of well-respected cryptography and computer science experts see no reason to advance attempts at creating access for the government.

Despite many scholar's views toward exceptional access, other notable literature demonstrates that some scholars do not close the door on a technically feasible solution for government access. A comprehensive report on encryption by the National Academies of Sciences, Engineering and Medicine examines several potential methods for permitting access for government agencies, all with varying degrees of technical feasibility.[28] Although all the options examined, like key escrow and vendor access, have significant technological, scale, or financial challenges, none were declared impossible.[29] Further, and like Ablon et al.'s findings, this report researched the future of encryption and the feasibility of continuing special access into the future.[30] Thus, what's the so what of it all?

Unlike the Ablon team's conclusions, the National Academies noted technologies in development that could both aid and impede government access. This report discusses a

[25] Hal Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* (Washington, DC: Center for Democracy and Technology, 2017), 13, https://doi.org/10.7916/D8GM8F2W.

[26] Ablon et al., *Going Dark*, 31.

[27] Ablon et al., 31.

[28] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate*, 58–66.

[29] National Academies of Sciences, Engineering and Medicine, 58–66.

[30] National Academies of Sciences, Engineering and Medicine, 66–67.

technology that would allow investigators to search encrypted data for certain keywords without revealing all the encrypted text, a highly useful tool if it were eventually able to be implemented.[31] The report also discusses the likely spread of encryption at the application level, which makes search warrants executed on mobile devices even more challenging.[32]

To the contrary, Stefan Savage, of the Department of Computer Science and Engineering at the University of California at San Diego, disagrees with conclusions that lawful access for law enforcement is technologically impossible without weakening encryption.[33] Savage, however, addresses device encryption only. Savage differs from the other authors in two ways. First, while the academics previously discussed state that lawful access is impossible without compromising the encryption itself, Savage asks whether such a technology can be designed that does not compromise encryption.[34] Second, Savage proposes a solution that stores decryption capabilities on a device itself.[35] A nefarious actor cannot scale Savage's proposed solution since possession of the device is required.[36] Also, Savage's proposal requires no changes to the encryption protocol, which eliminates the risk of creating software vulnerabilities that may be exploited on all devices.[37] Savage's proposal is important for highlighting that research into methods that provide for lawful access that still preserve as much security as possible may be worthwhile.

To summarize, a group of esteemed and accomplished experts in this field believe exceptional access is impossible or almost impossible, although not all agree that exceptional access to encryption is unattainable.

[31] National Academies of Sciences, Engineering and Medicine, 66–67.

[32] National Academies of Sciences, Engineering and Medicine, 67–68.

[33] Stefan Savage, "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion," in *CCS '18: 2018 ACM SIGSAC Conference on Computer and Communications Security* (New York: Association for Computing Machinery, 2018), 1761–62, https://cseweb.ucsd.edu/~savage/papers/lawful.pdf.

[34] Savage, 1762.

[35] Savage, 1761.

[36] Savage, 1762.

[37] Savage, 1762.

2. Alternatives to Search Warrants and Wiretaps

Many computer science experts agree that exceptional access weakens encryption, which, in turn, has many negative implications. Scholars in cryptography and other fields and those representing other perspectives have argued that alternatives exist for law enforcement and the IC that can be used in place of exceptional access. These alternatives, in their view, negate the need to enact legislation on the issue while giving law enforcement and the IC the information needed to succeed in their missions. Such alternatives ultimately allow the United States to maintain a posture of strong encryption.

One common alternative introduced by the literature is so-called lawful hacking; i.e., government agencies directing their efforts to exploit vulnerabilities in software and hardware that would allow those agencies to access evidence typically sought through a wiretap or search warrant directly. In literature that has explored lawful hacking in great detail, important aspects of the topic include the need for policies about agencies' responsibilities on reporting the vulnerabilities they find, ensuring that such activities are done within the legal bounds of the U.S. Constitution, and limiting the agencies' hacking activities to those spelled out in court-approved actions.[38]

Many, including some experts like Blaze and Landau who have also written about the need to maintain strong encryption, have proposed lawful hacking— and argue that it is a better option than creating "deliberate" weaknesses for exceptional access.[39] In agreement with Blaze and Landau, Hoathi Nguyen argues that lawful hacking represents a "middle-ground solution" that represents a compromise to the encryption debate.[40] A Georgetown Law Journal article examines various methods law enforcement uses to defeat encryption, which includes methods akin to hacking. The authors, Bruce Schneier and Orin Kerr, argue that encryption will only be a problem for criminal investigations if law

[38] Hoaithi Y. T. Nguyen, "Lawful Hacking: Toward a Middle-Ground Solution to the Going Dark Problem" (master's thesis, Naval Postgraduate School, 2017), 61–66, http://hdl.handle.net/10945/53024.

[39] Bellovin et al., "Lawful Hacking," 64.

[40] Nguyen, "Lawful Hacking," 78–79.

enforcement's "encryption workarounds" do not succeed.[41] The authors determine that whether encryption will be the game-changer that it is purported to be remains to be seen.[42] Overall, many scholars consider lawful hacking a legitimate alternative to granting law enforcement access.

A distinct body of literature proposes another avenue for intercepting data by law enforcement and the IC, the use of metadata, which, as these experts believe, eliminates the need to access data protected by encryption. Metadata, the data that accompanies files like location and device information, can provide a large amount of useful information that will never be encrypted because of its need to be accessed for proper routing, delivery, etc.[43] Others, including Krystle Kaul et al., call for a methodical approach to examining the use of metadata as an alternative considering that even accessing metadata may have negative implications for privacy.[44] Many experts view the vast troves of metadata as a new resource that can fill the gaps created by encryption. Metadata offers much useful information that does not require accessing any device or application that a user has opted to keep private.

3. Supporting Access for Law Enforcement

On the other hand, academic and computer science experts tend to agree on an important part of the encryption debate; that law enforcement has a legitimate need to access encrypted devices and messaging applications. Although they agree that the United States should continue to produce encryption products without access for law enforcement, they maintain that they are not anti-law enforcement. Despite some disagreement with the tone or terminology used by government officials, little of the literature on the subject suggests that law enforcement is not acting in good faith. In this context, Gasser et al. note

[41] Orin S. Kerr and Bruce Schneier, "Encryption Workarounds," *Georgetown Law Journal* 106 (2017): 14, https://doi.org/10.2139/ssrn.2938033.

[42] Kerr and Schneier, 14.

[43] Gasser et al., *Don't Panic*, 3.

[44] Krystle Kaul et al., *Going Darker 2.0: Policy Recommendations for Law Enforcement, the Intelligence Community and the Private Sector* (Washington, DC: DHS Office of Intelligence and Analysis, 2018), 5, https://www.dhs.gov/sites/default/files/publications/2018_AEP_Going_Darker_Phase2.pdf.

that they are not challenging the FBI's warnings about the dangers to public safety even though they may disagree with the scope of the problem.[45] These authors agree with the FBI that encryption is a "major challenge" for government agencies.[46] To summarize, the impetus that led many experts to publish their analyses is not an effort to stop or impede law enforcement, but to ensure that the integrity of encryption can continue to protect the data that needs protecting.

In the same context, some of the literature helps explain the challenges that the government faces in the wake of widespread adoption of encrypted technologies. One such challenge is the difficulty law enforcement, and even more so, intelligence agencies face due to the use of encrypted messaging applications by extremist groups. The literature highlights that encrypted messaging applications have become a major part of how groups like the Islamic State communicate. Indeed, as Alexander Meleagrou-Hutchens and Seamus Hughes note, the group's use of encrypted applications like Telegram has been called a "game changer" and has been found to play a significant role in its ability to encourage attacks in Western countries.[47] Encryption hinders intelligence collection that is an important element of national security.

Secure messages within terrorist groups are surely a challenge for intelligence agencies, although one group of scholars considers the problem somewhat greater for law enforcement than for the IC. The National Academies notes that members of the IC advise that the challenges faced are not as great as that of law enforcement.[48] Reasons for this lesser challenge may include the "more permissive" environment in which the IC operates, the greater amount of resources available to the IC, and the fact that intelligence professionals require a standard of proof less than that of reasonable doubt.[49] Thus, while

[45] Gasser et al., *Don't Panic*, 2.

[46] Ablon et al., *Going Dark*, vii.

[47] Alexander Meleagrou-Hitchens and Seamus Hughes, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs," *Combating Terrorism Center at West Point* 10, no. 3 (March 9, 2017): 1, https://ctc.usma.edu/wp-content/uploads/2017/03/CTC-Sentinel_Vol10Iss331.pdf.

[48] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate*, 8.

[49] National Academies of Sciences, Engineering and Medicine, 44.

the IC certainly faces challenges with this new technology, encryption has had a greater impact on law enforcement operations.

With that being said, literature on the scope of the challenge law enforcement faces both converges and diverges in its conclusions. In a 2017 report on encryption, the Congressional Research Service recognized that law enforcement's "investigative capabilities are outpaced by the speed of technological change."[50] Further, during a 2016 congressional hearing about encryption, the FBI noted that it "may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods" because of the negative effect encryption can have on its investigative techniques.[51] In a 2016 report, the House Committee on Homeland Security notes that encryption is having a negative impact on law enforcement's ability to prosecute cases successfully.[52] These articles represent the literature that reaches consensus on the scope of the challenge that law enforcement faces with encryption.

However, some scholars believe it is too early to label encryption a challenge for the government. Kerr and strong encryption advocate Schneier write that it is too early to decide what impact encryption will have on law enforcement until it is ascertained how effective workarounds will be.[53] If encryption can be easily defeated, then no challenge exists to overcome or regulate. Similarly, James A. Lewis et al. state that the issues that encryption causes for law enforcement are "manageable" and the "risks to public safety…[have] not reached the level that justifies restrictions."[54] In sum, no consensus

[50] Kristin M. Finklea, *Encryption and the 'Going Dark' Debate*, CRS Report No. R44481 (Washington, DC: Congressional Research Service, 2017), 1, https://crsreports.congress.gov/product/details?prodcode=R44481.

[51] Amy Hess, "Deciphering the Debate over Encryption," Federal Bureau of Investigation, April 19, 2016, https://www.fbi.gov/news/testimony/deciphering-the-debate-over-encryption.

[52] House Committee on Homeland Security, *Going Dark, Going Forward: A Primer on the Encryption Debate* (Washington, DC: House Committee on Homeland Security, 2016), 6, https://fas.org/irp/congress/2016_rpt/hsc-encrypt.pdf.

[53] Kerr and Schneier, "Encryption Workarounds," 14.

[54] Lewis, Zheng, and Carter, *The Effect of Encryption on Lawful Access to Communications and Data*, IV–V.

exists within the literature that law enforcement faces a challenge due to the encryption of devices and messaging applications.

4. Conclusion

Overall, many experts and academics on the subject of computer science and cryptography agree that the United States should not legislate away strong encryption. Nevertheless, the scientific community cannot fully agree on the right approach in dealing with encryption as it relates to law enforcement. Scientists and researchers who propose solutions or alternatives to lawful access tend to be drowned out by others who remain concerned that the United States is on a path of allowing weakened encryption, and thus increased vulnerabilities.

D. RESEARCH DESIGN

This thesis examines the problem of law enforcement being shut out of encrypted devices and applications and the debate surrounding such a lack of access. Law enforcement maintains that it must have access to encrypted communications by citing the public safety interest.[55] Cryptography and privacy experts maintain that law enforcement has adequate alternatives to meet its needs.

Scant available literature evaluates alternative accesses' potential effectiveness. To determine whether any offer a viable option for law enforcement, a policy options analysis is used. First, this thesis only evaluates alternatives suggested by experts in an academic field related to the debate, such as cryptology or law. Much of what has been written about the lawful access challenge has appeared in a wide variety of media sources, to include blogs, the news media, and advocacy organizations that cite or use works written by others, such as academics and experts. As a result, this thesis primarily focuses on the literature written by known and well-respected professionals who have spent much of their careers researching the issues related to encryption.

[55] "Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy," Department of Justice, October 10, 2017, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

Second, this thesis analyzes alternative policy options that have been proposed in the literature by scholars to solve the challenge. These policy options, if adopted by the government, would mean the government would no longer pursue access to encrypted devices and applications. Therefore, this thesis conducts a policy options analysis using criteria relevant to both sides of the debate. This analysis relies on four criteria in determining the viability of the options as adoptable policy:

- The policy solution preserves law enforcement's ability to develop evidence needed to prosecute criminals and terrorists.
- The policy solution protects civil rights and civil liberties.
- The policy solution preserves the United States' national security and public safety.
- The government's implementation of the policy solution is feasible.

Third, the aforementioned four criteria are applied to actual case studies and a hypothetical case study to determine the viability of the policy options introduced in the literature as law enforcement policy moving forward. Case studies, such as the 2015 terrorist attacks in San Bernardino, CA, help frame the debate by defining the stakeholders and their interests. The stakeholders include law enforcement, suspects, defendants, victims, and the communities where these acts occur. This thesis also employs a hypothetical case study to evaluate the alternatives to law enforcement access proposed by cryptology, privacy, and legal experts who secure sensitive law enforcement or victim information from being released. Such analysis further helps determine whether alternatives to law enforcement access can stand up in actual incidents in the place of encrypted data.

In my research, I consult the available literature on the government's position, consisting mostly of speeches and congressional testimony of law enforcement executives and reports, many from the U.S. Congress, which summarize law enforcement interests in the debate. Other sources include reports on local law enforcement's challenges with encryption, as well as criminal cases involving encryption in court action against criminal defendants. Research of these sources provides both context for law enforcement’s position in the debate, as well as its real-world scope. In addition, these sources aid the policy options analysis for this thesis, specifically as it relates to the effects of these policy options on criminal prosecutions. Several law enforcement executives have addressed this issue in their speeches and testimonies. Some have also cited specific criminal prosecutions, and I include those cases in my research, as well.

Chapter II provides a briefing on the history and technical aspects of encryption. Chapter III is a compilation of case studies that illustrate the lawful access challenge. Chapter IV provides a policy analysis of the alternatives to lawful access using the context demonstrated by the Chapter III case studies in determining the viability of the alternatives. Chapter V offers some recommendations for the debate moving forward, along with the thesis’ conclusion.

THIS PAGE INTENTIONALLY LEFT BLANK

II. AN INTRODUCTION TO THE ENCRYPTION DEBATE

As far back as the 1990s, law enforcement agencies in the United States had been raising the issue of the growing difficulty in obtaining evidence protected by commercial encryption. Many criminals, to include child pornographers, drug dealers, and terrorists, have used encryption to their advantage to keep evidence out of the reach of law enforcement and the IC. This tactic was once dubbed "going dark" by the FBI and is a phrase that has since been repeated by many.[56] Law enforcement is finding it increasingly difficult to access information because either technology companies encrypt data without retaining any capability to decrypt it or make devices so impenetrable that only a handful of incorrect passcode attempts will erase any important data it holds. Thus, court orders and search warrants are not useful because the data cannot be read. The FBI now refers to the challenge that "warrant-proof encryption" creates as the "lawful access challenge."[57] The block of lawful access is an increasingly pressing and urgent problem for American law enforcement. For example, FBI Director Christopher Wray reported in early 2018 that the FBI encountered approximately 1,200 mobile devices in fiscal year 2017 that it could not access due to encryption despite having the legal authority to do so.[58] Thus, encryption cripples law enforcement's investigatory efforts.

Society is becoming increasingly digitized, and information is now found on devices that need passcodes or facial scans to open that people often stored in drawers or under beds in the past. As a result, in a debate over the use of encryption, law enforcement argues for its need for lawful access to encrypted data while privacy advocates, cryptographers, and technology companies argue for strong encryption practices without allowances for the government, with warrants or not. These groups fear that requiring programs or processes that allow government access will weaken encryption because those

[56] Comey, "Going Dark."

[57] Federal Bureau of Investigation, "The Lawful Access Challenge."

[58] Dustin Volz, "FBI Says No Misconduct in Inflated Number of Encrypted Phones," *Wall Street Journal*, sec. Politics, May 23, 2018, https://www.wsj.com/articles/fbi-says-no-misconduct-in-inflated-number-of-encrypted-phones-1527113031.

with nefarious intent may develop the capability to exploit those programs or processes that may also facilitate lawful access for law enforcement.[59]

This chapter introduces the debate on the types of encryption encompassed in the phrase going dark, including a briefing on its technical aspects, a history of the debate itself including its origins, and a familiarization with the parties involved. This debate is often described as privacy versus security. This chapter explains why it is more appropriate to refer to this debate as public safety versus information security.

A. ENCRYPTION EXPLAINED

Encryption is certainly nothing new. In fact, Julius Caesar created a method of encrypting messages that only the sender and receiver could understand because only those two had the key to decrypt the message.[60] Anyone who intercepted the message could not understand it because it appeared to be nonsense. This subterfuge happened more than 2,000 years ago. Today, encryption is not much different except that it occurs electronically. Once data is encrypted, it appears as cipher text similar to the unreadable nonsense of Caesar's time. Whoever possesses the electronic key converts the cipher text to readable data, which is called plaintext.[61] In this way, what seems new actually mimics historical practice.

The encryption debate focuses on access to plaintext. Law enforcement agencies argue they cannot access plaintext data despite having a court order—usually either a search warrant or a communications intercept order—because of either file-based encryption or end-to-end encryption. In the context of this thesis, file-based encryption and full-disk encryption refer to the encryption of a mobile device, like a smartphone. For several years, smartphones have been encrypted by a protocol known as full-disk

[59] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate*, 1–8.

[60] "Encryption and Public Keys," Khan Academy, accessed June 9, 2019, video, 6:39, https://www.khanacademy.org/computing/computer-science/internet-intro/internet-works-intro/v/the-internet-encryption-and-public-keys.

[61] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate,* 15–16.

encryption. This type of encryption secures the user's data on a device and the program files of the operating system. Full-disk encryption became a widespread practice in 2014 when technology companies began using it on mobile devices by default.[62] Typically, a device protected by this form of encryption will erase all data on the device when too many incorrect passcodes have been entered. Recently, file-based encryption has been replacing full-disk encryption as the standard for smartphones. As the name suggests, file-based encryption means that files are encrypted by their own systems. In contrast, end-to-end encryption secures data passed between two-parties so that only the sender and the receiver can see the communications. This thesis examines (1) file-based and full-disk encryption as mobile device encryption, and (2) end-to-end encryption as communications encryption as the two primary access issues in the encryption debate.

These types of encryption secure two types of data that law enforcement seeks access to, data at rest and data in motion. Data at rest is stored on devices protected by passcodes, like iPhones and Android smartphones, and mobile device encryption. Data in motion refers to communications between two persons communicating via a messaging application that encrypts the messages between the two, i.e., end-to-end encryption, and contains no other access to read the messages. The lawful access challenge refers to the situation in which law enforcement finds itself with these two types of encrypted data.[63]

1. Data at Rest

So what prevents law enforcement from accessing data at rest protected by encryption? A modern iPhone can store voluminous amounts of data at rest because Apple has built hardware encryption into the device, as well as something Apple calls "data protection."[64] When an iPhone user establishes a passcode for the device, it automatically authorizes data protection.[65] Then, if a subject tries to access an iPhone via a brute-force

[62] Finklea, *Encryption and the 'Going Dark' Debate*, 5.

[63] Federal Bureau of Investigation, "The Lawful Access Challenge."

[64] "Data Protection Overview," Apple, Inc., accessed August 17, 2020, https://support.apple.com/guide/security/data-protection-overview-secf6276da8a/1/web/1.

[65] "Passcodes," Apple, Inc., accessed August 17, 2020, https://support.apple.com/guide/security/passcodes-sec20230a10d/1/web/1.

attack, trying possible combinations of passcodes, the phone wipes all its data after a set number of unsuccessful attempts, often ten.[66] To make any attempts even more difficult, Apple employs "escalating time delays" starting on the fifth attempt for entering different passcodes, which increase to an hour required between attempts after the eighth one.[67] Therefore, if someone is trying to access a device via brute force, it may take in excess of five years to do so if the passcode is a six-digit combination of letters and numbers.[68] Notably, such encryption is not limited to Apple devices. Other phone manufacturers, such as Motorola, also provide similar device encryption capability.[69] Thus, the technology itself resists access to data at rest.

The latest of the iPhone's operating systems offers access with Touch ID (fingerprint scanning) or Face ID (facial recognition).[70] On phones programmed for Touch ID or Face ID, the passcode still reigns supreme for access to the phone because if a user fails to unlock the phone with Face ID or Touch ID after five attempts, the phone reverts to requiring the passcode for unlocking.[71] What is especially challenging to law enforcement and beneficial to owners of such devices is that having Face ID or Touch ID encourages a user to create a particularly complex and lengthy passcode since users rarely have to enter it.[72]

2. Data in Motion

Whereas device encryption is keeping law enforcement from accessing at rest data on those devices, law enforcement is also struggling to access real-time communications taking place via encrypted messaging applications. One of the most popular of these

[66] Apple, Inc.

[67] Apple, Inc.

[68] Apple, Inc.

[69] "Data Encryption," Motorola, accessed June 6, 2019, https://support.motorola.com/in/en/solution/MS98572.

[70] "Touch ID, Face ID, Passcodes, and Passwords," Apple, Inc., accessed August 17, 2020, https://support.apple.com/guide/security/touch-id-face-id-passcodes-and-passwords-sec9479035f1/1/web/1.

[71] Apple, Inc.

[72] Apple, Inc.

encrypted messaging applications is WhatsApp, with over one billion users worldwide.[73] Like many other encrypted applications, WhatsApp uses end-to-end encryption so only the sender and the receiver of the message have the ability to decrypt the message.[74]

In a February 2017 report produced by the Center for Strategic and International Studies, authors James Lewis, Denise Zheng, and William Carter predicted that by 2019, 22 percent of instant messages sent globally on all messaging apps would be encrypted end-to-end.[75] Lewis et al. refer to a Juniper Research report that finds that more than 100 trillion messages were sent in 2016 alone.[76] Therefore, it can deduced that globally, trillions and trillions of messages sent via applications with end-to-end encryption are out of the reach of interception by law enforcement agencies. Other popular applications using end-to-end encryption include Telegram, a messaging service that also allows users to send photo and video files, and Viber, a messaging application that started offering end-to-end encryption in 2016.

B. EVOLUTION OF THE DEBATE ON ENCRYPTION

Beginning with the Clipper Chip and the resulting Crypto Wars, the modern debate on encryption has made access, for better or for worse, the main issue. It has evolved from a debate over modifying devices with the Clipper Chip to requiring access to inaccessible data.

1. The Clipper Chip

One item originally seen as a potential solution in the history of the encryption debate was the Clipper Chip.[77] This product, originally designed by the National Security Agency, was a device for telephones that had a program that allowed law enforcement

[73] “About WhatsApp,” WhatsApp, accessed June 6, 2019, https://www.whatsapp.com/about/.

[74] Andy Greenberg, “Hacker Lexicon: What Is End-to-End Encryption?,” Wired, November 25, 2014, https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

[75] Lewis, Zheng, and Carter, *Effect of Encryption on Lawful Access to Communications and Data*, 7–8.

[76] Lewis, Zheng, and Carter, 7.

[77] Spinello, *Cyberethics*, 219–21.

agencies to intercept and understand encrypted communications.[78] This capability also pitted the government against a variety of groups including privacy advocates and technology companies in what has been labeled the "Crypto Wars," the onslaught of groups that fought to stop the chip's implementation.[79] The Clipper Chip had a backdoor designed to be accessible to two agencies of the U.S. government.[80] When a Clipper Chip phone was used, it would emit data specifically for U.S. law enforcement agencies, which with a valid court order, would then obtain the needed access from the two U.S. government agencies (each had a required access key) holding the keys in escrow. Then, law enforcement would be able to unencrypt and intercept the communications.[81] Thus, the technology had built-in access for law enforcement.

The government pursued the Clipper Chip technology as the "industry standard for encryption," and the FBI viewed it as a way to provide privacy protections while still allowing law enforcement to conduct lawful surveillances of communications without the hurdle of encryption.[82] Eventually, the Clipper Chip turned out to have vulnerabilities that dissuaded its implementation.[83] Matt Blaze of AT&T Bell Laboratories discovered that the chip could be used without transmitting the data the government needed to unencrypt the data.[84] Nonetheless, the Clipper Chip had a backdoor intended specifically for the government to use. Such access is significant today because some scholars compare the lawful access that law enforcement seeks to the nature of what would have been permitted with the Clipper Chip.

[78] Spinello, 219–21.

[79] Danielle Kehl, Andi Wilson, and Kevin Bankston, *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s* (Washington, DC: New America, 2015), 3–15, https://static.newamerica.org/attachments/3407--125/Lessons%20From%20the%20Crypto%20Wars%20of%20the%201990s.882d6156dc194187a5fa51b14d55234f.pdf.

[80] Spinello, *Cyberethics,* 219.

[81] Spinello 219.

[82] Spinello, 219–21.

[83] Finklea, *Encryption and the 'Going Dark' Debate,* 4.

[84] Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard," in *CCS94: 2nd ACM Conference on Computer & Communications Security* (New York: Association for Computing Machinery, 1994), 59–67, https://doi.org/10.1145/191177.191193.

2. CALEA

Although the FBI began discussing the encryption issue on the public stage much more frequently beginning in 2014, the legislative and law enforcement history in dealing with this issue goes back much further. In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA).[85] This act directs telecommunications carriers to "enable" the government to intercept communications by ensuring its facilities can allow such action when presented with a court order.[86] CALEA applies to certain telecommunications providers but not to others that may be pertinent to this debate.[87] Perhaps most notably in regards to the encryption debate, the statute specifically requires that telecommunications carriers must be able to decrypt or facilitate the decryption of data that has been encrypted by the carrier's customers unless the carrier encrypted the data and thus can decrypt it itself.[88] CALEA ensures that law enforcement agencies can intercept communications in an evolving technological environment without having to invest heavily in skills, equipment, or technology to do so.

Importantly, CALEA does not apply to many of the types of companies today that provide messaging applications using end-to-end encryption like Facebook with WhatsApp or Snap, Inc. that owns the Snapchat platform.[89] CALEA defines telecommunications carriers narrowly to certain, more established types of providers like telephone companies.[90] It does not include "over-the-top" applications that operate independently of internet service providers, which include popular messaging applications.[91] In 2004, Congress expanded CALEA to require compliance for companies

[85] Lewis, Zheng, and Carter, *The Effect of Encryption on Lawful Access to Communications and Data*, 36.

[86] "Title 47 U.S. Code § 1002—Assistance Capability Requirements," Legal Information Institute, accessed June 6, 2019, https://www.law.cornell.edu/uscode/text/47/1002.

[87] Legal Information Institute.

[88] Legal Information Institute.

[89] Lewis, Zheng, and Carter, *The Effect of Encryption on Lawful Access to Communications and Data*, 36.

[90] Lewis, Zheng, and Carter, 36.

[91] Lewis, Zheng, and Carter, 36.

that include "online voice communications" among their services.[92] However, this expansion preceded the popularity of companies that make messaging applications with end-to-end encryption.[93] Neither changes to CALEA nor the Federal Communications Commission's (FCC's) interpretation of the act since 2004 have changed, nor has any new legislation been passed specifically in reference to messaging applications and interception.

3. CESA

Several years after the Clipper Chip died, the Clinton administration took the next major stab at finding a solution to law enforcement's challenges with encryption when it proposed legislation titled the Cyberspace Electronic Security Act of 1999 (CESA). In a message to Congress on September 16, 1999, President Clinton cited "significant and heretofore unseen challenges to law enforcement and public safety" as a reason for proposing the act.[94] One of the major elements of the act sought to "allow access to plaintext by law enforcement when encryption is utilized by criminals."[95] The legislation called for third-party recovery agents to be responsible for holding decryption keys.

On the same day President Clinton sent his message to Congress advocating for the proposed legislation, the White House issued a report titled *Preserving America's Privacy and Security in The Next Century: A Strategy for America in Cyberspace*.[96] This document, authored by the Secretaries of Defense and Commerce, the Attorney General, and the

[92] Hugh J. McCarthy, "Decoding the Encryption Debate: Why Legislating to Restrict Strong Encryption Will Not Resolve the 'Going Dark' Problem," *Journal of Internet Law* 20, no. 3 (September 2016): 20–21, ProQuest.

[93] "OMB Approves CALEA Compliance Monitoring Report for Providers of Facilities-Based Broadband Internet Access and Interconnected VOIP Service; Reports Are Due February 12, 2007," Federal Communications Commission, December 14, 2006, https://www.fcc.gov/document/omb-approves-calea-compliance-monitoring-report-providers-facilities.

[94] Cyberspace Electronic Security Act of 1999--Message from the President of the United States, H. Doc. 106–123, 106th Cong., 1st sess., *Congressional Record* 145, no. 123 daily ed. (September 21, 1999): H8390–91, https://www.congress.gov/congressional-record/1999/9/21/house-section/article/H8390-8.

[95] Cyberspace Electronic Security Act of 1999.

[96] William Cohen et al., *Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace* (Washington, DC: The White House, 1999), https://fas.org/irp/news/1999/09/990916-crypto-wh.htm.

Director of the Office of Management and Budget, outlined the White House's policy toward cybersecurity, including its stance on the encryption debate.[97] In alignment with the White House's proposed legislation on encryption, the document called for recovery agents to maintain decryption tools that allow law enforcement access with a valid court order, and the creation and funding of a law enforcement "Technical Support Center."[98] This center would research encryption and methods of accessing encrypted data and protections for proprietary information shared by private sector companies with law enforcement agencies.[99] Congress neither considered nor ever passed the bill.[100]

The proposed legislation in CESA resembled the proposal of the national standardization using the Chipper Chip in that it sought to have custodians hold the keys in escrow until they were needed by law enforcement, which essentially created an exception for law enforcement to have access to decrypted data.[101] In addition, an element of the CESA proposal, specifically the funding of the Technical Support Center, parallels a common alternative offered by scholars to encourage law enforcement access to devices without compromising encryption standards.

C. ENCRYPTION STRENGTHENS

The Crypto Wars were short-lived, but the debate would eventually be renewed in the mainstream after the Snowden disclosures and other major events led to a push for more privacy for technology users. The more recent events fueled a move to widespread encryption due to user concerns about the safety and privacy of personal information.

[97] Cohen et al.

[98] Cohen et al.

[99] Cohen et al.

[100] Tricia E. Black, "Taking Account of the World as It Will Be: The Shifting Course of U.S. Encryption Policy," *Federal Communications Law Journal* 53, no. 2 (2001): 305, https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1271&context=fclj.

[101] Black, 309–10.

1. Concerns over Mass Surveillance

In 2013, classified documents began to be leaked to the media by an NSA contractor named Edward Snowden. Snowden obtained about 1.5 million classified documents from government networks that detailed multiple surveillance programs aimed at people worldwide, including Americans.[102] The documents he downloaded also included secret documents produced by foreign allies. The documents revealed that the NSA, with the cooperation of numerous technology and telecommunications companies, had amassed voluminous databases of information about the companies' customers. The disclosures became a major media story and reactions from citizens around the globe were strong. As a result, companies like Apple and Google took notice and started marketing products that had strong security protocols, including specifications like end-to-end encryption.[103]

Several years later, Snowden remains a household name while facing criminal charges in the United States but also has been considered by many as a whistleblower and hero, who has won awards for leaking the documents. Furthermore, the information Americans learned about government surveillance programs revealed in the documents he leaked has been the impetus for the development of a market where companies and entrepreneurs promote a wide range of products and services that ensure an individual's privacy.[104]

2. Encryption by Default

Apple and Google had the answer to the fear generated by Snowden's leaks. A year after the leak, in 2014, Apple and Google announced they would make encryption the default standard for iPhones with Apple iOS 8 and Android smartphones running the Android L operating systems.[105] The iOS and Android operating systems account for the

[102] House Permanent Select Committee on Intelligence, *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden* (Washington, DC: U.S. Government Publishing Office, 2016), i, https://www.congress.gov/114/crpt/hrpt891/CRPT-114hrpt891.pdf.

[103] Constantinos Patsakis et al., "The Market's Response toward Privacy and Mass Surveillance: The Snowden Aftermath," *Elsevier* 73 (2018): 194–96, https://doi.org/10.1016/j.cose.2017.11.002.

[104] Patsakis et al., 195.

[105] Miller, "Google and Apple Encrypt by Default."

overwhelming majority of market share for smartphones worldwide, which was nearly 99% by the end of 2019.[106] Now that the two most common operating systems were implementing encryption without smartphone owners activating it, law enforcement faces an encryption challenge on a much larger scale than it had previously seen. Since neither Google nor Apple maintains possession of the keys needed to unlock the encrypted devices, law enforcement has no way to access these devices despite having court orders to do so.

Moving toward default encryption as the standard continues. The most recent major move came in April 2019 when Facebook confirmed that it was working toward default end-to-end encryption for its Facebook Messenger application.[107] Facebook has indicated the change will take years but has pledged to enact the feature in the future.[108] This messaging application is one of the most popular, with 1.3 billion users worldwide as of 2017.[109] Soon after default encryption became the norm, an important smartphone featuring default encryption would make the encryption debate a major headline.

3. San Bernardino: A Seminal Event

On December 2, 2015, at about 11:00 am, Syed Rizwan Farook and his wife, Tashfeen Malik, entered the Inland Regional Center where the San Bernardino Office of Public Health, Farook's employer, was holding an office party.[110] Later in the morning, Farook and Malik, armed with AR-15 rifles, came into the party dressed in tactical gear,

[106] S. O'Dea, "Mobile Operating Systems' Market Share Worldwide from January 2012 to December 2019," Statista, February 28, 2020, https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/.

[107] Nicole Lee, "Facebook Messenger Is Getting Faster, Lighter and More Secure in 2019," *Engadget*, April 30, 2019, https://www.engadget.com/2019/04/30/facebook-messenger-f8-2019/.

[108] Andy Greenberg, "Facebook Says Encrypting Messenger by Default Will Take Years," Wired, January 10, 2020, https://www.wired.com/story/facebook-messenger-end-to-end-encryption-default/.

[109] J. Clement, "Facebook Messenger—Statistics and Facts," Statista, June 25, 2019, https://www.statista.com/topics/4625/facebook-messenger/.

[110] Elinson and Frosch, "San Bernardino Shooting."

and began shooting.[111] In the end, Farook and Malik fired somewhere between 65 and 75 rounds, killed 14 people, and injured another 21 people.[112]

Immediately, the FBI and its Joint Terrorism Task Force, along with state and local law enforcement agencies, began investigating and doing so at what the Assistant Director in Charge of the FBI's Los Angeles Office described as "breakneck speed."[113] Eventually, investigators found Farook's county-owned iPhone in his mother's car.[114] As noted earlier, this phone would become the epicenter of the debate on encryption and law enforcement's ability, or lack thereof, to access encrypted devices.

The legal battle over the encrypted phone began in February 2016 when the DOJ applied for a court order in the U.S. District Court for the Central District of California requiring the iPhone's maker, Apple, Inc., to help the FBI access Farook's phone.[115] The iPhone had a security feature that would wipe the phone's data if too many incorrect passcodes were entered.[116] Specially, the department sought to compel Apple to design software that would allow the FBI to enter in as many passcodes as needed to guess the correct code eventually without wiping the phone.[117] A U.S. Magistrate Judge granted the order compelling Apple's assistance.[118] On the same day, Apple's CEO, Tim Cook, issued a letter to Apple's customers explaining that Apple would refuse to comply with the court's

[111] Elinson and Frosch.

[112] "Timeline: The San Bernardino Shooting and Aftermath Step by Step," *Los Angeles Times*, December 6, 2015, https://www.latimes.com/visuals/graphics/la-g-san-bernardino-shooting-timeline-20151204-htmlstory.html.

[113] "San Bernardino Press Conference with FBI," December 7, 2015, PBS Newshour, video, 15:09, https://www.pbs.org/newshour/nation/watch-live-san-bernardino-press-conference-with-fbi.

[114] "Everything We Know about the San Bernardino Terror Attack Investigation," *San Bernardino Sun*, November 27, 2016, https://www.sbsun.com/2016/11/27/everything-we-know-about-the-san-bernardino-terror-attack-investigation/.

[115] In the Matter of the Search of an iPhone Seized during the Execution of a Search Warrant of a Black Lexus IS300, California License Plate 35KGD203, No. ED 15–0451M (C.D. Cal. 2016), 1, https://www.justice.gov/usao-cdca/file/825001/download.

[116] In the Matter of the Search of an iPhone Seized during the Execution of a Search Warrant of a Black Lexus IS300, California License Plate 35KGD203, 2.

[117] In the Matter of the Search of an iPhone Seized during Execution of a Search Warrant of a Black Lexus IS300, California License Plate 35KGD203, 2.

[118] In the Matter of the Search of an iPhone Seized during the Execution of a Search Warrant of a Black Lexus IS300, California License Plate 35KGD203, 1–3.

order.[119] Cook argued that the government was asking Apple to create a backdoor to Apple's encryption operating system that Cook called "too dangerous to create."[120]

What ensued was a court battle between the DOJ and Apple, with several other technology companies coming to Apple's support, about enforcing or vacating the initial court order.[121] Eventually, a third party assisted the FBI in accessing Farook's iPhone, which thus made Apple's cooperation unnecessary and ended the case without a definitive answer as to whether the Magistrate Judge's decision would have withstood Apple's legal challenge.[122] If an answer had been provided, the encryption debate may look entirely different today.

4. Cambridge Analytica and Privacy

Years later, with several major privacy compromises making the news, including the breach of the federal Office of Personnel Management, another major privacy compromise became public. In 2018, reports surfaced that a political consulting firm called Cambridge Analytica had obtained sensitive personal data about as many as 87 million Facebook users in 2014 using an application called "thisisyourdigitallife."[123] Due at least in part to poor data protection practices by Facebook, Cambridge Analytica successfully acquired vast amounts of data on Facebook users from a personality test in the application that such users had completed.[124] Even more unsettling for many was that Cambridge Analytica had even obtained data on Facebook users who had not used the application but were friends with users who had taken the personality test.[125] The scandal, which led to a $5 billion fine against Facebook in a settlement with the Federal Trade Commission, also

[119] Cook, "Customer Letter."

[120] Cook.

[121] Elizabeth Weise, "Apple v FBI Timeline: 43 Days That Rocked Tech," *USA Today*, March 15, 2016, https://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400/.

[122] "Everything We Know about the San Bernardino Terror Attack Investigation."

[123] Ikhlaq ur Rehman, "Facebook-Cambridge Analytica Data Harvesting: What You Need to Know," *Library Philosophy and Practice*, 1–11, 2019, https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5833&context=libphilprac.

[124] ur Rehman.

[125] ur Rehman.

included the disclosure that Cambridge Analytica had used the data it mined to target individuals with information designed to influence the 2016 U.S. presidential campaign.[126] Facebook has almost 2.4 billion monthly users.[127] Considering this staggering figure, unsurprisingly, this story has impelled the desire for companies that store significant amounts of personal data about its users to have strong privacy protocols. In all likelihood, many Americans think of such scandals when considering whether privacy and security matter in the digital platforms and products they use.

5. The EARN IT Act

A current legislative proposal would afford immunity from prosecution to companies in exchange for their taking action against malign actors who use their platforms for child sexual abuse. The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (the EARN IT Act) introduced in the U.S. Senate on March 5, 2020 represents one of the latest proposed legislations that would affect encryption.[128] If passed, the act would no longer allow technology companies to be shielded by a law that protects websites from being held liable for certain materials that appear on their platforms.[129] The members of Congress who introduced the bipartisan bill state that the bill provides a mechanism to encourage technology companies to take action against child sexual abuse material.[130] In exchange for doing so, compliant companies receive safe harbor from lawsuits related to material the companies' users transmit through the companies' services.[131] Currently, technology companies already (mostly) have a safe harbor, without

[126] ur Rehman.

[127] "Facebook Reports First Quarter 2019 Results," Facebook, April 24, 2019, https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-First-Quarter-2019-Results/default.aspx.

[128] "Graham, Blumenthal, Hawley, Feinstein Introduce EARN IT Act to Encourage Tech Industry to Take Online Child Sexual Exploitation Seriously," United States Senate Committee on the Judiciary, March 5, 2020, https://www.judiciary.senate.gov/press/rep/releases/graham-blumenthal-hawley-feinstein-introduce-earn-it-act-to-encourage-tech-industry-to-take-online-child-sexual-exploitation-seriously.

[129] United States Senate Committee on the Judiciary.

[130] United States Senate Committee on the Judiciary.

[131] United States Senate Committee on the Judiciary.

conditions, as set forth in Section 230 of the Communications Decency Act of 1996.[132] Under the new proposal, companies can adopt a set of best practices, to be determined by a commission and approved by Congress, to earn and maintain their safe-harbor immunity.[133] Ultimately, the EARN IT Act forces companies to address the ramifications their encryption protocols can have on the children who appear in images of child pornography traded on the internet.[134]

The EARN IT Act is a response to an issue that New York has said to be at a "breaking point."[135] The proliferation of child pornography traded on the internet has increased astronomically with reports to the National Center for Missing and Exploited Children increasing more than 18 times in four years, from 1 million in 2014 to over 18 million in 2018.[136] It is made possible not only by the technologies that make trading this material easier, but also at least in part by the technology companies that have failed to devote resources to address the issue on their platforms.[137] End-to-end encryption also has played a large role in the ability of child pornography to proliferate on the internet.[138]

Nonetheless, the bill has attracted concern because companies that use end-to-end encryption cannot easily scan content transmitted via their platforms for child pornography because communications between users on these platforms cannot be decrypted. For this reason, such companies cannot comply with wiretap orders involving their users. This

[132] Riana Pfefferkorn, "The EARN IT Act: How to Ban End-to-End Encryption without Actually Banning It," *The Center for Internet and Society* (blog), January 30, 2020, http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it.

[133] United States Senate Committee on the Judiciary, "Graham, Blumenthal, Hawley, Feinstein Introduce EARN IT Act."

[134] Stewart Baker, "The EARN IT Act Raises Good Questions about End-to-End Encryption," *Lawfare* (blog), February 11, 2020, https://www.lawfareblog.com/earn-it-act-raises-good-questions-about-end-end-encryption.

[135] Michael H. Keller and Gabriel J. X. Dance, "The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?," *New York Times*, sec. U.S., September 29, 2019, https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

[136] Keller and Dance.

[137] Keller and Dance.

[138] Keller and Dance.

protection would likely make it difficult for companies using end-to-end encryption to comply with the best practices for preventing the transmission of child pornography.

Some argue that the EARN IT Act is a de facto way of regulating end-to-end encryption because it requires technology companies to enact best practices to prevent the transmission of child pornography on their platforms, which is technically unlikely because companies cannot access user transmissions.[139] Cryptographers like Bruce Schneier and Johns Hopkins University Professor Mathew Green have linked the EARN IT Act with Attorney General Barr's criticisms of end-to-end encryption, with Green calling the act a "backdoor" attempt to ban encryption.[140] Along with the Electronic Frontier Foundation (EFF) and numerous technology media companies, Green and Schneier have referred to this act as a cunning way to ban end-to-end encryption because the legislation holds companies liable for child pornography on their platforms that they cannot surveil.

At the time of this writing, the EARN IT Act is still a proposal in Congress. Nonetheless, the issue of the relationship between child pornography and end-to-end encryption is an important one for the encryption debate. It is a relationship receiving less attention than the one between encryption and terrorism even though it is much more widespread.[141] This relationship also continues to worsen considering the continued growth of reports of child pornography by technology companies. As the proliferation of child pornography continues, it will become more and more difficult to defend the sanctity of end-to-end encryption.[142]

D. THE ENCRYPTION DEBATE: THE PARTIES

The encryption debate is often described as having two sides, security and privacy, but more than two participants engage in this debate. The security side encompasses law

[139] Pfefferkorn, "The EARN IT Act."

[140] Bruce Schneier, "The EARN-IT Act," *Schneier on Security* (blog), March 13, 2020, https://www.schneier.com/blog/archives/2020/03/the_earn-it_act.html.

[141] Susan Hennessey, *The Elephant in the Room: Addressing Child Exploitation and Going Dark*, Aegis Paper Series (Stanford, CA: Hoover Institution, Stanford University, 2017), 1–3, https://www.hoover.org/sites/default/files/research/docs/hennessey_webreadypdf.pdf.

[142] Hennessey, 1–3.

enforcement and the IC (collectively, the government). The privacy side constitutes privacy advocates, computer scientists and cryptographers (collectively, the technology experts), and technology companies. This section identifies the major parties in the encryption debate, their interest in the debate, and their position on the widespread implementation of encryption.

1. The Government: Fighting Going Dark

Since the widespread adoption of default encryption by operating system makers, law enforcement has made two key points in its argument for access, judicial orders grant law enforcement access to encrypted data, but technology companies thwart such access, and the result threatens public safety. In 2014, FBI leadership began speaking publicly about the encryption issue. That year then FBI Director James Comey told attendees at an event at the Brookings Institution in Washington, DC that even with lawful authority, many public safety professionals often cannot fulfill their missions because of their "lack of technical ability to do so."[143] This lack is what Comey referred to when he first coined the term "going dark" as he was specifically addressing the difficulty faced when trying to access encrypted data.[144] In 2019, while speaking at the International Conference on Cyber Security, Attorney General William P. Barr further discussed the going dark issue when he told conference attendees that the risk to public safety is increasing because of the refusal of technology companies to provide lawful access to encrypted data.[145] In these ways, law enforcement is a paper tiger, toothless to acquire full information on known threats.

Yet another group has a significant stake in this debate, the IC. This group's goals generally align with federal law enforcement agencies' mission of protecting the homeland.[146] The IC has been stymied over the past several years by terrorists who have used encrypted platforms to talk to one another. With less insight into terrorist

[143] Comey, "Going Dark."

[144] Comey.

[145] "Australia Passes Encryption-Breaking Laws," BBC News, December 7, 2018, https://www.bbc.com/news/world-australia-46463029.

[146] "Mission," Office of the Director of National Intelligence, accessed March 15, 2020, https://www.intelligence.gov/mission.

communications, the IC has found itself in circumstances in which it has had less awareness of terrorist activity, recruiting, planning, etc. Congressman Adam Schiff, currently the chairman on the House Permanent Select Committee on Intelligence, noted in a statement regarding the 2015 Paris terrorist attacks that Islamic State of Iraq and Syria (ISIS) members use platforms that have encryption as a feature. This encryption, according to Schiff's statement, creates "significant security, technological, economic and privacy issues" for law enforcement and the IC.[147] In a 2016 letter to Senator Ron Wyden, the Office of the Director of National Intelligence called encryption a "significant impediment" to the IC's ability to achieve its mission.[148] The IC is a paper tiger, too.

2. The Privacy Advocates

Historically, two organizations have been at the forefront of the encryption debate on the side of arguing for strong encryption without access for law enforcement, the EFF and the American Civil Liberties Union (ACLU). Founded in 1990, the EFF bills itself as "the leading nonprofit organization defending civil liberties in the digital world."[149] When it comes to privacy, the EFF's website notes that "respect for individuals' autonomy, anonymous speech, and the right to free association must be balanced against legitimate concerns like law enforcement."[150] Dating back to 1920, the ACLU calls itself "our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties."[151] Over the years, both organizations have had roles in the debate over encryption.

[147] "Intelligence Committee Ranking Member Schiff Statement on Encryption Debate in Wake of Paris Attacks," United States House of Representatives Permanent Select Committee on Intelligence, November 18, 2015, https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=196.

[148] Katie Bo Williams, "Intelligence Community Pushes Back on Encryption Report," The Hill, May 9, 2016, https://thehill.com/policy/cybersecurity/279231-intelligence-community-pushes-back-on-pro-encryption-report.

[149] "About EFF," Electronic Frontier Foundation, accessed June 7, 2019, https://www.eff.org/about.

[150] "Privacy," Electronic Frontier Foundation, accessed June 7, 2019, https://www.eff.org/issues/privacy.

[151] "About the ACLU," American Civil Liberties Union, accessed June 7, 2019, https://www.aclu.org/about-aclu.

Both the ACLU and the EFF spoke out against the Chipper Clip in the 1990s, and thus solidified their roles in the Crypto Wars. The ACLU compared the chip to forcing construction companies to put surveillance devices in homes under construction.[152] The founder of the EFF, John Perry Barlow, argued that it could lead to widespread surveillance.[153] Barlow also argued at one point that requiring a specific encryption standard, as the Clipper Chip would have done, violates the First Amendment of the U.S. Constitution that protects both American's content and manner of speech.[154]

In 2004, as the FCC was considering expansion of CALEA, the EFF came out in opposition to the new rules that the FCC proposed. The EFF stated that the FCC was requiring broadband internet and Voice over Internet Protocol providers to build "insecure backdoors" that "will also endanger the privacy of innocent people, stifle innovation, and risk the Internet as a forum for free and open expression."[155]

3. The Technology Experts

As noted in Chapter I, computer scientists and cryptographers have been especially outspoken about the dangers of law enforcement access. Collaborative works with respected scientists and scholars like Susan Landau, Bruce Schneier, and Matt Blaze have emphasized the position of many in the field that access for law enforcement is fraught with dangers.[156] Further, these experts have been at the forefront of arguing for the need to implement alternatives to law enforcement access, such as permissible hacking of encrypted devices and applications, using metadata, and court-ordered disclosure of passcodes by defendants. Subsequent chapters explore these issues in greater detail.

[152] Spinello, *Cyberethics*, 220.

[153] Spinello, 220.

[154] John Perry Barlow, "A Plain Text on Crypto Policy," Electronic Frontier Foundation, September 6, 1993, https://www.eff.org/pages/plain-text-crypto-policy.

[155] Rebecca Jeschke, "Plan for Internet 'Backdoors' Draws Coordinated Attack," Electronic Frontier Foundation, October 26, 2005, https://www.eff.org/deeplinks/2005/10/plan-internet-backdoors-draws-coordinated-attack.

[156] Gasser et al., *Don't Panic*, 1–15.

4. Technology Companies

Technology companies have been participants in the encryption debate since the Crypto Wars. The proposal of the Clipper Chip was one of the first challenges the industry made against government action on encryption. Major technology companies like NCR, Compaq, and IBM, represented by the Computer and Business Equipment Manufacturers Association, argued that the chip would hurt the companies' abilities to compete overseas.[157] This point has been raised in the current debate as well.[158]

The Snowden disclosures emboldened the technology industry to favor the use of strong encryption. Companies like Google and Microsoft criticized U.S. and UK government counterterrorism surveillance programs and vowed not to cooperate with requests from agencies like the National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ).[159] Snowden has been the impetus for the technology industry moving toward more and stronger encryption for their products.[160] This motivation emerged not out of an ideological position on privacy protection, but rather an economic motive for companies introducing products with strong security protocols, including specifications like end-to-end encryption.[161]

Technology companies have also spoken out in opposition to encryption limits in other western nations, to include the United Kingdom and Australia. In the United Kingdom, technology companies including Apple, Microsoft, and Google penned a letter, along with privacy advocates and security experts, dismissing a proposal by the GCHQ that would have allowed the GCHQ to insert "ghost" users into chat rooms for surveillance

[157] John Markoff, "Computer Code Plan Challenged," *New York Times*, May 29, 1993, http://timesmachine.nytimes.com/timesmachine/1993/05/29/924093.html.

[158] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate*, 81–82.

[159] Robin Simcox, *Surveillance after Snowden: Effective Espionage in an Age of Transparency* (London: The Henry Jackson Society, 2015), 61–65, http://henryjacksonsociety.org/wp-content/uploads/2015/06/Surveillance-After-Snowden-16.6.15.pdf.

[160] Simcox, 61–65.

[161] Patsakis et al., "The Market's Response toward Privacy and Mass Surveillance," 194–96.

purposes.[162] In Australia, technology industry lobbyist DIGI, which represents companies like Google and Facebook, criticized a new law aimed at requiring law enforcement access to locked smartphones, stating that the measure will result in greater risk to public safety.[163] These arguments resemble those of the ACLU, the EFF, and cryptography experts like Bruce Schneier.

In contrast, many of the same companies have cooperated with governments in other places, particularly Russia and China. In Russia, Apple has agreed to comply with Russian law by storing customer data within Russian borders, which makes that data available, requires a company to maintain customer communications for at least six months, and requires the information be turned over to government agencies upon request.[164] Like Russia, China requires that certain operations of technology companies be located in China, which led to Apple moving encryption keys and iCloud data to the country after Apple formed a partnership with a Chinese technology company that has strong ties to the government there.[165] Apple revealed that it has turned over some customer data to the Chinese government in the past.[166]

Ironically, laws restricting technology and internet use, like communications, are significantly more restrictive in Russia and China than in democratic nations like the United States. Democracy think tank Freedom House, which produces an annual report on internet freedom titled "Freedom on the Net," rated China and Russia as "not free" while

[162] Government Communications Headquarters, *Open Letter to GCHQ* (Cheltenham, United Kingdom: Government Communications Headquarters, 2019), 1–2, https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf.

[163] DIGI, *Submission to the Parliamentary Joint Committee on Intelligence and Security on the Telecommunications and Other Legislation Amendment (Assistance and Access Bill) 2018* (Canberra, Australia: DIGI, 2018), 1–2, https://digi.org.au/advocacy/.

[164] "Russia: 'Big Brother' Law Harms Security, Rights," Human Rights Watch, July 12, 2016, https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

[165] Shannon Liao, "Apple Officially Moves Its Chinese ICloud Operations and Encryption Keys to China," *The Verge*, February 28, 2018, https://www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accounts-government-privacy-speed.

[166] Liao.

the United States was rated "free."[167] In this way, technology companies support the goals of autocratic governments that repress their own people but refuse to cooperate with lawful warrants in the United States. Perhaps it simply represents that the customer, the power-end-user, demands encryption in the United States, whereas technology companies can only operate in certain foreign countries with government permission, which makes the government the powerful customer there.

However, not all technology companies have cooperated with laws that affect encryption in countries outside the United States. Shortly after Russia's data storage law came into effect, popular messaging application Telegram, which uses end-to-end encryption for text messages and voice calls over the internet, was ordered to hand over its encryption keys to the Russian government.[168] When Telegram said it could not because it did not have the keys, a Russian court approved a request to block access to the application in Russia by Roskomnadzor, which is Russia's agency responsible for media and communications.[169] In 2020, reports surfaced that Russian legislators proposed a halt on the ban to allow for health-related communications by government agencies during the COVID-19 pandemic.[170]

In China, the mainland blocks the Telegram application, yet users based in Hong Kong can access it. In 2019, Telegram revealed publicly that it had been a victim of a cyberattack by China.[171] Telegram further noted that the attack coincided with protests in Hong Kong against a Chinese law allowing persons to be extradited to mainland China for

[167] Adrian Shahbaz and Allie Funk, *Freedom on the Net 2019: The Crisis of Social Media," Freedom on the Net* (Washington, DC: Freedom House, 2019), 14–15, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.

[168] "Russia to Block Telegram over Encryption," BBC News, April 13, 2018, https://www.bbc.com/news/technology-43752337.

[169] Andrew Roth, "Russia Blocks Millions of IP Addresses in Battle against Telegram App," *The Guardian*, sec. World news, April 17, 2018, https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app.

[170] Helen Partz, "Russia May Lift Telegram Ban Due to Coronavirus Outbreak," Cointelegraph, April 23, 2020, https://cointelegraph.com/news/russia-may-lift-telegram-ban-due-to-coronavirus-outbreak.

[171] Associated Press, "Chinese Cyberattack Hits Encrypted Messaging App Used by Hong Kong Protesters," *New York Post*, June 13, 2019, https://nypost.com/2019/06/13/chinese-cyberattack-hits-encrypted-messaging-app-used-by-hong-kong-protestors/.

judicial actions.[172] In this way, some companies have pushed back against government access to encrypted devices just as they have done in the United States.

E. CONCLUSION

The encryption debate pits the need for security against the individual's right to privacy. Government agencies seek to access encrypted data in the name of public safety and homeland security. Privacy advocates, computer scientists, and technology companies resist government access to encrypted data in the name of privacy and cybersecurity. Many call for the need to strike a balance between the two interests. Susan Landau, however, defines the debate differently, and more accurately, as being safety versus security.[173] Such a debate pits public safety against information security, both of which, when compromised, can have significant implications for U.S. security. Regardless, law enforcement executives have argued their stance for years as a need to stop threats to U.S. security, and encryption as threatening their ability to do that.

[172] Associated Press.

[173] Mark Bohannon, "The State of Encryption: How the Debate Has Shifted," Opensource.com, June 13, 2018, https://opensource.com/article/18/6/listening-susan-landau.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE NEED FOR ACCESS TO ENCRYPTED DATA FOR LAW ENFORCEMENT AND THE U.S. INTELLIGENCE COMMUNITY

As this thesis analyzes potential policy options for addressing encryption, establishing the legitimate need for law enforcement and the IC to access encrypted data is important. Law enforcement's need is more transparent given the public and domestic nature of their mission and activities, although the IC often operates in a domain that requires much greater protection of information. In law enforcement, police seek evidence of criminal activity to establish the probable cause required to arrest offenders. Prosecutors seek to convict those offenders by presenting proof beyond a reasonable doubt where the proceedings are made public. In contrast, the IC analyzes sources of information to inform government leaders on appropriate courses of action in furtherance of America's foreign policy objectives, often in a classified setting shielded entirely from public view. Information presented in this chapter is based on available public reporting relevant to both fields.

The public debate on encryption often takes place in the context of terrorism and child sexual exploitation. However, encryption stymies investigations of a wide variety of crimes and agencies seek encrypted data for a wide variety of reasons. Police may seek to identify terrorists or prevent terror attacks. They may be trying to rescue victims of crimes like human trafficking, child sexual exploitation, or kidnapping. Sometimes they are looking for data that will provide clues in murders, narcotics trafficking, or large-scale fraud. Decrypted data may be evidence that helps prosecute an offender or exonerate an innocent person. The IC's needs for accessing encrypted data are likely narrower in scope and difficult to articulate because of the operational needs of keeping information secret. Nonetheless, this chapter presents case studies that illustrate the needs for lawful access by both. These case studies were chosen for their availability to unrestricted information, the importance of the role digital information played in the case, and the mix of both domestic and foreign terror attacks, as well as domestic crimes. The case studies are supplemented by other information that provides important context to underscore the importance of lawful access to encrypted data.

A. THE MISSION DEMONSTRATES THE NEED FOR ACCESS

For this nation's security agencies, public safety and maintaining the security of the homeland are at the core of their missions. The Los Angeles Police Department's mission statement, for example, references the need "to enhance public safety," while the Chicago Police Department states that it is "committed to protect[ing] the lives, property and rights of all people."[174] The New Jersey State Police notes in its mission statement that it "ensure[s] public safety."[175] The U.S. Secret Service defines part of its mission as the need to "minimize and decisively respond to identified threats and vulnerabilities."[176] The Central Intelligence Agency (CIA) includes in its mission the need to "preempt threats."[177] Former Deputy Attorney General Rod Rosenstein once noted that the government needs certain tools to accomplish its security mission, like search warrants and communications interceptions.[178] Without access to these things, agencies lose important tools that ensure they can carry out their security and protection missions.

Since the terror attacks of September 11, 2001, counterterrorism has been a focus of law enforcement and intelligence agencies worldwide. The United Nations, in its counterterrorism strategy, recognizes that terrorism seeks to undo human rights, dismantle democracy, and threaten the security and stability of sovereign states, and calls for the international community to fight it.[179] Groups like Al Qaeda and the Islamic State have taken credit for attacks on American soil and against American interests. Information that

[174] "The Mission Statement of the LAPD," Los Angeles Police Department, accessed March 18, 2020, http://www.lapdonline.org/inside_the_lapd/content_basic_view/844; "Mission," Chicago Police Department, accessed March 18, 2020, https://www.chicago.gov/content/city/en/depts/cpd/auto_generated/cpd_mission.html.

[175] "Mission Statement," New Jersey State Police, accessed March 18, 2020, https://www.njsp.org/about/mission-statement.shtml.

[176] "The Protective Mission," United States Secret Service, accessed August 17, 2020, https://www.secretservice.gov/protection/.

[177] "CIA Vision, Mission, Ethos & Challenges," Central Intelligence Agency, November 1, 2018, https://www.cia.gov/about-cia/cia-vision-mission-values.

[178] Department of Justice, "Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy."

[179] United Nations General Assembly, *The United Nations Global Counter-Terrorism Strategy* (New York: United Nations, 2006), 2, https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy.

is important to law enforcement in investigating and preventing these attacks is often found on cell phones instead of being in closets, under the bed, or hidden away in the attic. Correspondence, contact lists, mapping, videos, etc., are important pieces of evidence for law enforcement and are increasingly digitized on personal mobile devices. In addition, such devices are becoming ubiquitous. In the United States, 81% of those over the age of 18 owned a smartphone by the end of 2018.[180]

In addition, people are using a variety of applications to send and receive messages more than ever. It is estimated that as many as 2.52 billion persons worldwide used mobile messaging applications in 2019, and the number is growing.[181] Telegram, one of the most popular messaging applications that offers end-to-end encryption, boasted 200 million active users in 2018, with up to 700,000 new users a day.[182] Criminals and terrorists are following the trends along with the rest of the world in relying more and more on digital communications and devices. The following section is a study of the importance of digital information to security and law enforcement agencies.

B. ELECTRONIC COMMUNICATIONS

Terrorist attacks are often high profile, and sometimes world-changing events. Often valuable information is contained in communications between terrorists and on the mobile devices that attackers own and use for these events. Encryption has made it more and more difficult to access terrorists' information. Security services worldwide seek information to prevent and disrupt attack planners and terror cells. The following case studies illustrate instances when communications were intercepted or when encryption prevented agencies from intercepting communications between nefarious actors. In addition, this section examines a case in which investigators were delayed in accessing valuable and actionable intelligence because of encryption.

[180] S. O'Dea, "Smartphone Ownership Rate by Country 2018," Statista, February 27, 2020, https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/.

[181] J. Clement, "Mobile Messaging Users Worldwide 2018–2022," Statista, October 8, 2019, https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/.

[182] Pavel Durov, "200,000,000 Monthly Active Users," Twitter, March 28, 2018, 11:35 a.m., https://twitter.com/durov/status/979034229052006400.

1. Interception before Encryption

Evidence derived from intercepting communications can be invaluable for disrupting and preventing terror attacks. However, measuring these successes can be challenging because of the lack of public details about how, or even if, attacks have been prevented including instances where intercepting electronic communications aided in such prevention.[183] Many intelligence officials and terrorism experts agree that intelligence successes that have thwarted attacks often cannot be discussed in public forums, while the failures are well documented.[184] The two case studies presented in this section, both of which have been made public, illustrate the importance the content of intercepted communications can play in disrupting terror plots. Both events transpired before encryption was an issue for those in the security sector.

a. Europe (2007)

In 2007, the Austrian government initiated a counterterrorism investigation against a subject named Mohammed Mahmoud, which included intercepting Mahmoud's internet chat sessions.[185] The content of Mahmoud's discussions that the Austrian government intercepted included talk of launching an attack in Europe using explosives.[186] One of the people Mahmoud discussed the attack with was Said Namouh who lived in Canada.[187] Namouh and Mahmoud discussed detailed plans to conduct a suicide attack in Europe with Namouh planning to act as the suicide bomber.[188] This information led to an investigation in Canada that found that Namouh was actively communicating with jihadists around the world, including having conversations related to the kidnapping of a journalist by the Army

[183] Erik J. Dahl, "The Plots that Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks against the United States," *Studies in Conflict & Terrorism* 34, no. 8 (August 1, 2011): 622, https://doi.org/10.1080/1057610X.2011.582628.

[184] Dahl, 622–23.

[185] United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (Vienna: United Nations, 2012), 86, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

[186] United Nations Office on Drugs and Crime, 86.

[187] United Nations Office on Drugs and Crime, 86.

[188] United Nations Office on Drugs and Crime, 87.

of Islam, a U.S. designated terrorist organization.[189] The details of these conversations were also obtained through intercepts.[190]

By late 2007, authorities had intercepted 31 conversations the two had about conducting an attack in Europe.[191] Authorities in both countries decided to disrupt the planning and arrested both subjects in their home countries. In finding Namouh guilty, the court specifically cited the intercepted communications as a major factor in the verdict.[192] The ability of counterterrorism authorities to be able to intercept Mahmoud's communications was directly responsible for disrupting Namouh's attack. Had Mahmoud been using an end-to-end encrypted application instead, the Austrian government never would have been able to intercept those chats, never would have connected Mahmoud to Namouh, and an attack would very well have killed many.

b. United States (2009)

Another success because of intercepts of communications by security agencies happened in 2009. Federal agents arrested Najibullah Zazi in Colorado following an investigation that determined that Zazi traveled to New York City with the intent of conducting an attack using explosives and had purchased components of the explosive triacetone triperoxide (TATP).[193] Zazi was arrested after a Queens man, Ahmad Wais Afzali, was approached by police detectives in New York City seeking information from Afzali, which led Afzali to tip off Zazi about the police investigating his actions.[194] Zazi had something in common with someone who had been arrested several months earlier in the United Kingdom.[195] Abid Naseer had also plotted a terror attack, specifically in the

[189] United Nations Office on Drugs and Crime, 86–87.

[190] United Nations Office on Drugs and Crime, 87.

[191] United Nations Office on Drugs and Crime, 86–87.

[192] United Nations Office on Drugs and Crime, 87–88.

[193] "Najibullah Zazi Indicted for Conspiracy," Department of Justice, September 24, 2009, https://www.justice.gov/opa/pr/najibullah-zazi-indicted-conspiracy.

[194] "Three Arrested in Ongoing Terror Investigation," Department of Justice, September 20, 2009, https://www.justice.gov/opa/pr/three-arrested-ongoing-terror-investigation.

[195] Raffaello Pantucci, "Manchester, New York and Oslo," *CTC Sentinel* 3, no. 8 (August 1, 2010): 12, https://ctc.usma.edu/wp-content/uploads/2010/10/CTCSentinel-Vol3Iss8-13.pdf.

UK city of Manchester.[196] Naseer and Zazi were connected in that both had contact with an email account of someone named “Ahmad” with whom both Naseer and Zazi had discussed terror plots.[197]

In 2009, UK police arrested Naseer and several others linked to Al Qaeda after Naseer’s email communications had been intercepted and were found to contain discussions about attack plans using explosives.[198] After the arrests of Naseer and his associates, the UK’s Crown Prosecution Service (CPS) determined it could not move forward with prosecuting the group due to a lack of evidence.[199] This decision would lead to an examination of the investigation and arrests that lead to several recommendations about how the CPS and police communicate during counterterrorism investigations.[200] However, UK’s immigration court, which examined Naseer’s immigration status after his release from police custody, determined that Naseer was indeed an Al Qaeda operative based on examination of Naseer’s intercepted emails.[201] The email interceptions also led to the detection of Zazi’s actions in the United States and the subsequent foiling of that plot by his arrest in Colorado.[202] Had Naseer been using an encrypted mobile application like those available today, explosives attacks may well have occurred in 2009 in Manchester, England and New York City because police may never have detected the plans discussing them.

[196] Pantucci, 12.

[197] Pantucci, 12.

[198] Pantucci, 10–11.

[199] Alex Carlile, *Operation Pathway: Report Following Review* (London: Independent Reviewer of Terrorism Legislation, 2009), 14, https://webarchive.nationalarchives.gov.uk/20100416131809/http://security.homeoffice.gov.uk/news-publications/publication-search/legislation/terrorism-act-2000/operation-pathway-report.

[200] Carlile, 19–20.

[201] *Abid Naseer, Ahmad Faraz Khan, Shoaib Khan, Abdul Wahab Khan and Tariq ur Rehman v. Secretary of State for the Home Department*, No. SC/77/80/81/82/83/09 (Special Immigration Appeals Commission 2010), 10–11, https://www.legislationline.org/download/id/3976/file/UK_Special%20Immigration%20Appeals%20Commission%20_Judgement_2010.pdf.

[202] Pantucci, “Manchester, New York and Oslo,” 11.

2. Interception Efforts after Encryption

Significant evidence today indicates that terrorists now use end-to-end encryption to obfuscate their communications. Such encryption provides a sort of communications safe haven for terrorists to talk to each other in a way that law enforcement, the IC, foreign governments, and even the companies that offer these products cannot detect what they are discussing. Islamic State terrorists who use encrypted communications indeed have been involved in attacks or planned attacks in the homeland.[203] The case studies presented next, both involving the Islamic State, illustrate how encryption has stymied counterterrorism investigations to the point of an attack being carried out.

a. The Islamic State in Syria (2015)

One such Islamic State member was Junaid Hussain. Hussain was a member of a group of computer savvy Islamic State members who spoke English. The group, known as "the Legion," also included fellow Islamic State members Reyaad Khan and Neil Prakash.[204] Hussain specialized in internet propaganda and recruitment for the Islamic State.[205] Hussain was also a user of encrypted communications and specifically used Surespot.[206] Surespot is a messaging application that uses end-to-end encryption and ensures its users that "not even the Surespot server, can view the contents of the data" sent through its application.[207]

Hussain was a threat to the U.S. homeland not just because of his use of the internet to spread propaganda and recruit members, but also especially because of his ability to assist recruits in planning, plotting, and carrying out attacks in America. One such recruit was Munir Abdulkader who was convicted in 2016 of terrorism offenses after having

[203] Meleagrou-Hitchens and Hughes, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs," 1.

[204] Nafees Hamid, "The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain," *CTC Sentinel* 11, no. 4 (April 26, 2018): 34, https://ctc.usma.edu/wp-content/uploads/2018/04/CTC-SENTINEL-042018-3.pdf.

[205] Hamid, 34.

[206] Hamid, 34.

[207] "How Surespot Works," Surespot, accessed March 21, 2020, https://www.surespot.me/documents/how_surespot_works.html.

regular contact with Hussain.[208] At the direction and encouragement of Hussain, Abdulkader planned to murder a U.S. government employee and fire Molotov cocktails at an Ohio police station.[209] The murder plot included plans to kidnap the government employee, behead that employee, and film the assassination.[210] The plot involved taking significant steps to carry it out, including training and obtaining ammunition.[211]

Abdulkader, who had also been in contact with an FBI informant, was eventually arrested after he took the step of trying to buy an AK-47 rifle.[212] Abdulkader had initially conveyed his support for Islamic State of Iraq and the Levant (ISIL) in Twitter messages before eventually having contact with the FBI informant and Hussain.[213] Hussain was known to be a user of Surespot and it is known that he had communicated at least some of the time with Abdulkader via an encrypted messaging application.[214] In this instance, law enforcement arrested Abdulkader thanks to the involvement of the informant who was able to make contact with Abdulkader and in whom Abdulkader had confided. Unfortunately, law enforcement could not disrupt some attacks because U.S.-based attackers were using encrypted messaging applications.

b. The Islamic State in the United States (2015)

Such an attack happened in 2015 when two men, Elton Simpson and Nadir Soofi, traveled to an event center in Garland, TX that was hosting a “Draw Mohammed Contest” event that had been organized by a group founded by anti-Muslim advocate Pamela Geller. The two opened fire outside of the event and both were killed by local police. Before that

[208] “Cincinnati-Area Man Pleads Guilty to Plot to Attack U.S. Government Officers,” Department of Justice, July 7, 2016, https://www.justice.gov/opa/pr/cincinnati-area-man-pleads-guilty-plot-attack-us-government-officers.

[209] Department of Justice.

[210] *United States v. Munir Abdulkader*, No. 1:16-CR-019, 68 (S.D. Ohio October 9, 2018), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/AbdulkaderSentencingProceedings.pdf.

[211] Department of Justice, “Cincinnati-Area Man Pleads Guilty to Plot to Attack U.S. Government Officers.”

[212] Department of Justice.

[213] Department of Justice.

[214] Meleagrou-Hitchens and Hughes, “The Threat to the United States from the Islamic State’s Virtual Entrepreneurs,” 3.

attack happened, Simpson had been in regular contact with an ISIS recruiter over the internet, including communications that occurred between the two over Surespot.[215] That recruiter, Mohamed Abdullahi Hassan, also known as Mujahid Miski, had left the United States to join the Somali terrorist group Al-Shabaab. Hassan left that group in 2013 and later became associated with ISIS while he was still in Somalia.[216] After the shooting, the FBI revealed that Simpson traded 109 encrypted messages with an "overseas terrorist," although it has not been released if this person was Miski or not.[217] It is known that the FBI had investigated Simpson in the past and an undercover FBI special agent was even following him on the day of the attack. The undercover agent, however, was not aware that Simpson intended to attack the event.[218] It is reasonable to surmise that, had Simpson been using an unencrypted communications platform that morning, the FBI may have been able to prevent the attack because they could have accessed the messages he was sending to and receiving from a terrorist.

3. The Struggle to Gain Access: Pensacola, FL (2019)

The following case study contains some parallels to the San Bernardino attack in that investigators could not access the attacker's cell phone because it employed full-disk encryption. However, unlike with the San Bernardino event, the U.S. government has made public at least some of the valuable information found on the device used in Pensacola when investigators were able to access the phone.

This incident occurred on December 6, 2019 on the grounds of the Pensacola Naval Air Station. On this day, a pilot in the Saudi Royal Air Force who was attending a training

[215] Anderson Cooper, "60 Minutes Investigates First ISIS-Claimed Attack in U.S. and What the FBI Knew," 60 Minutes, March 26, 2017, https://www.cbsnews.com/news/terrorism-in-garland-texas-what-the-fbi-knew-before-the-2015-attack/.

[216] Meleagrou-Hitchens and Hughes, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs," 2.

[217] James Eng, "FBI Director: Encrypted Messages Stymied Probe of 'Draw Muhammad' Shooting," NBC News, December 9, 2015, https://www.nbcnews.com/tech/security/fbi-director-encrypted-messages-stymied-probe-garland-shooting-n477111.

[218] Todd Shepherd, "Judge Dismisses Lawsuit Alleging FBI Role in 2015 Terror Attack in Texas," *Washington Free Beacon*, January 5, 2019, https://freebeacon.com/issues/judge-dismisses-lawsuit-alleging-fbi-role-in-2015-terror-attack-in-texas/.

program for members of foreign militaries arrived at the base but then launched an attack when he brandished a gun and began shooting.[219] The shooter, Second Lt. Mohammed Saeed Alshamrani, killed three members of the U.S. Navy in the attack.[220] In a subsequent press conference, the U.S. Attorney General called the shooting a terrorist act and reported that Alshamrani had expressed jihadist and anti-American views on social media and had recently visited the 9/11 Memorial in New York.[221] Al Qaeda in the Arabian Peninsula (AQAP) later claimed responsibility for the attack in a video the group released in February 2020.[222] According to AQAP, Alshamrani had spent much time at different U.S. bases with the intention of finding the best target, and he tied the shooting to other AQAP-linked terror attacks including an Al Shabaab attack on a joint Somali-American military base.[223] The AQAP representative in the video called Alshamrani a hero and encouraged other Muslims in the United States to launch attacks.[224]

Alshamrani brought more than a pistol and plenty of ammunition to the naval station on December 6th. He also carried two iPhones.[225] During the shooting, the gunman apparently damaged both phones. One even had a bullet shot through it, but law enforcement still repaired both phones to the point of being operational.[226] The FBI obtained a search warrant to search the phones; however, both iPhones were encrypted and, as the Attorney General announced more than a month after the shooting, neither phone

[219] William P. Barr, “Attorney General William P. Barr Announces the Findings of the Criminal Investigation into the December 2019 Shooting at Pensacola Naval Air Station,” Department of Justice, January 13, 2020, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-findings-criminal-investigation-december-2019.

[220] Barr.

[221] Barr.

[222] Thomas Joscelyn, “AQAP Claims ‘Full Responsibility’ for Shooting at Naval Air Station Pensacola,” *FDD’s Long War Journal*, February 2, 2020, https://www.longwarjournal.org/archives/2020/02/aqap-claims-full-responsibility-for-shooting-at-naval-air-station-pensacola.php.

[223] Joscelyn.

[224] Joscelyn.

[225] Barr, “Attorney General William P. Barr Announces the Findings of the Criminal Investigation into the December 2019 Shooting at Pensacola Naval Air Station.”

[226] Barr.

could be accessed by law enforcement.[227] The Attorney General noted that a goal of searching the phones was to determine whether Alshamrani had engaged in communications with any persons before his death, and equally important, what he may have discussed.[228] Surely, the subsequent claims made by AQAP regarding the attack have made this need seem even greater.

Several months later, Attorney General Barr announced that the FBI had been able to gain access to Alshamrani's phone despite Apple's unwillingness to help.[229] Investigators successfully defeated security features on one of the phones that contained valuable evidence.[230] Among the information mined from the phone was intelligence regarding an al-Qaeda member with whom Alshamrani had prior contact, as far back as 2015.[231] The data gleaned from the device was used in a CIA operation targeting the member in Yemen, which was effective in weakening that member's cell.[232]

Although this case may demonstrate that law enforcement on occasion may be able to access devices despite full-disk and file-based encryption, FBI Director Wray, standing with the Attorney General, highlighted that the FBI initially tried to access the phone several months prior because it needed the data then.[233] Barr also pointed out that the ability to access this single phone was not indicative of the FBI possessing a "scalable solution" to the going dark problem.[234] This case illustrates the need for widespread lawful access that can be executed in a timely manner.

[227] Barr.

[228] Barr.

[229] Katie Benner and Adam Goldman, "F.B.I. Finds Links between Pensacola Gunman and Al Qaeda," *New York Times*, sec. U.S., May 18, 2020, https://www.nytimes.com/2020/05/18/us/politics/justice-department-al-qaeda-florida-naval-base-shooting.html.

[230] Benner and Goldman.

[231] Benner and Goldman.

[232] Pete Williams, "FBI: Pensacola Gunman Prodded by Al Qaeda to Attack," NBC News, May 18, 2020, https://www.nbcnews.com/news/us-news/fbi-pensacola-gunman-prodded-al-qaeda-attack-n1209276.

[233] Benner and Goldman, "F.B.I. Finds Links between Pensacola Gunman and Al Qaeda."

[234] Benner and Goldman.

4. Transmitting Child Pornography: Collier County, FL (2020)

In June 2020, the police in Collier County, FL arrested a subject, who was a sheriff's deputy there, for possessing child pornography.[235] The subject, Rashaad Aubrey Smith, was charged with 100 counts after he was found to have numerous images on a computer in his home containing a file folder named "Porn."[236] Smith initially came under suspicion when the National Center for Missing and Exploited Children (NCMEC) became aware of the transmission of suspicious images determined to be of young boys engaging in sexual acts through the Skype application.[237] Companies like Skype Technologies, owner of the application, have been required to report "known incidents" of child pornography to the NCMEC since Congress amended the Victims of Child Abuse Act in 1998.[238] In addition to the images reported to NCMEC, police found images of children as young as 3-years old engaged in sex acts.[239] Following the arrest, Smith was fired from his law enforcement position.

NCMEC has discussed publicly the negative effect that end-to-end encryption has on detecting cases like Smith's since the encryption protocol makes it impossible for a service provider to detect such images.[240] NCMEC estimates that service provider reports regarding child pornography will decline substantially as end-to-end encryption is widely adopted.[241]

[235] Michael Braun, "Collier Deputy Arrested; Report Says Search at Home Finds 100 Instances of Child Porn," *Fort Myers News-Press*, June 14, 2020, https://www.news-press.com/story/news/crime/2020/06/14/collier-county-deputy-facing-100-counts-child-pornography/3187134001/.

[236] Braun.

[237] Braun.

[238] Kathryn C. Seigfried-Spellar, Gary R. Bertoline, and Marcus K. Rogers, "Internet Child Pornography, U.S. Sentencing Guidelines, and the Role of Internet Service Providers," in *Digital Forensics and Cyber Crime*, ed. Pavel Gladyshev and Marcus K. Rogers (Berlin, Heidelberg: Springer Berlin Heidelberg, 2012), 25, https://www.researchgate.net/publication/285975958_Internet_Child_Pornography_US_Sentencing_Guidelines_and_the_Role_of_Internet_Service_Providers.

[239] Braun, "Collier Deputy Arrested."

[240] "NCMEC's Statement Regarding End-to-End Encryption," National Center for Missing and Exploited Children, October 3, 2019, https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption.

[241] National Center for Missing and Exploited Children.

C. SMART PHONE DATA GENERALLY

Today's smartphones can store large amounts of data and allow users to conduct all sorts of transactions. In addition to video and photo capability, the smartphone has replaced many things that someone may have kept in a drawer at home or on their desk at work. These functions include correspondence, contact lists, photo albums, videos, financial records, purchase records, appointment books, to-do lists, and so on. Not only can smartphone devices do so much, but they also have become ubiquitous. Over 421 million mobile devices are in the United States, more than one per person.[242] In addition, mobile data use is surging among those mobile devices. The wireless industry saw an increase of 82% in data use from 2017 to 2018.

Data extracted from cell phones often yields vital evidence in criminal investigations of a wide variety of acts. Child sexual exploitation cases, particularly involving the distribution of child pornography, are often discussed in tandem with law enforcement's need to access encrypted data. However, decrypting data also is essential in the investigation of murders, kidnapping, fraud, etc. This section examines the importance of accessing digital evidence and the impediments created when police cannot. Presented are cases that relied on digital evidence for the successful investigation and conviction of offenders, yet they are also examples of cases that stymied investigators because of encryption.

1. Manhattan DA: Child Sexual Exploitation (2017)

Few local law enforcement agencies discuss the issues they experience with full-disk encryption and the challenges that arise. The New York County District Attorney's Office in Manhattan, NY (Manhattan DA) is one of the few. This agency has compiled reports of its experiences with full-disk encryption annually since 2015, shortly after default encryption for most smartphones became popular. These reports give insight into the totality of the issue the Manhattan DA faces, as well as documentation on several individual cases investigated and prosecuted at the local level.

[242] "2019 Annual Survey Highlights," CTIA, June 20, 2019, https://www.ctia.org/news/2019-annual-survey-highlights.

One such case in which evidence extracted from a smartphone proved vital involves the arrest and prosecution of Milton Narvaez. Narvaez was the subject of an investigation by the Manhattan DA for possessing and sharing child pornography over the internet.[243] Investigators seized his smartphone and secured a search warrant for the device. Although the phone was encrypted, investigators accessed the device with assistance from a paid consultant.[244] The phone held evidence on it that Narvaez was involved in much more than just the sharing of child pornography files. Narvaez also was found to have raped two children, including one whom he employed to babysit for a period of over six years starting from when the child was just six years old.[245] The other victim, whom investigators were unable to identify, was raped by Narvaez in a storage room at a church where Narvaez worked as a janitor. Investigators found video recordings on Narvaez's smartphone that he had made of his assaults of these children.[246] Narvaez was found guilty of the child sex assault and child pornography charges following a trial in 2017.[247] Like in many cases of this nature, digital evidence was the primary evidence indicating wrongdoing. If investigators had not been able to access Narvaez's phone, he may never have been charged with his crimes.

2. Manhattan DA: The Statistics

In a 2019 report on mobile device encryption, the Manhattan DA identified seven categories of criminal investigations in which a mobile device had been seized as part of

[243] "DA Vance: Babysitter Convicted at Trial for Sexually Assaulting Two Children," Manhattan District Attorney's Office, November 28, 2017, https://www.manhattanda.org/da-vance-babysitter-convicted-trial-sexually-assaulting-two-children/.

[244] Cy Vance, "Written Testimony for the United States Senate Committee on the Judiciary on Smartphone Encryption and Public Safety," Manhattan District Attorney's Office, December 10, 2019, https://www.manhattanda.org/written-testimony-for-the-united-states-senate-committee-on-the-judiciary-on-smartphone-encryption-and-public-safety/.

[245] Manhattan District Attorney's Office, "DA Vance."

[246] Manhattan District Attorney's Office.

[247] Manhattan District Attorney's Office.

the investigation.[248] Categories enumerated in that report include the crimes of homicide, sex offenses, narcotics, and identity theft.[249] While the media often focuses on the headline cases in which encrypted phones are impeding investigations into terrorism and mass shootings, impenetrable mobile devices, and to a lesser extent end-to-end encryption, often interrupt investigations into every major crime that police departments are responsible for investigating.

In 2019 testimony before the U.S. Senate Judiciary Committee, Manhattan DA Cy Vance told senators that criminals' use of mobile devices to plan, discuss, and carry out crimes was the biggest challenge his office has faced in recent memory.[250] While Vance cited a success story in this regard with Narvaez's prosecution, he cited another example of a sex trafficking investigation in which the suspect indicated he was aware of his device's default encryption settings and the benefit that provided for him because the police were unable to access the device.[251] Vance's testimony confirms that because of the suspect's understanding of the device's encryption settings, the office's sex trafficking investigation cannot progress.[252]

Not only can evidence from a cell phone contain information that can identify victims and help convict violent offenders, but it can also be used to exclude suspects and exonerate the accused. In the Manhattan DA's report on encryption for 2018, the office found 17 instances where evidence extracted from a smartphone exonerated someone.[253] In one case detailed by the Manhattan DA, witnesses had identified two defendants as being

[248] Manhattan District Attorney's Office, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: October 2019* (New York: Manhattan District Attorney's Office, 2019), 5, https://www.manhattanda.org/wp-content/uploads/2019/10/2019-Report-on-Smartphone-Encryption-and-Public-Safety.pdf.

[249] Manhattan District Attorney's Office, 5.

[250] Vance, "Written Testimony for the United States Senate Committee on the Judiciary on Smartphone Encryption and Public Safety."

[251] Vance.

[252] Vance.

[253] Manhattan District Attorney's Office, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: November 2018* (New York: Manhattan District Attorney's Office, 2018), 5, https://www.manhattanda.org/wp-content/uploads/2018/11/2018-Report-of-the-Manhattan-District-Attorney27s-Office-on-Smartphone-En....pdf.

involved in a gang assault.[254] Examination of data from one of the defendants' smartphones led to the finding that these two defendants were not only innocent of any assault, but were not even present at the time of the incident.[255] Despite the successes, many investigations end without justice being served because of encryption, particularly through the use of full-disk and file-based encryption.

3. Baton Rouge, LA Homicide (2015)

Vance's office is not alone in the frustration experienced with investigations stymied by encryption. In 2015, Brittany Mills was 29-years old and late in her pregnancy with her second child when she was shot in her doorway in Baton Rouge, LA.[256] Mills died shortly after the child was born via cesarean section, but the child only survived for three days.[257] Homicide investigators obtained information regarding Mills' smartphone usage, including toll records and phone data stored on iCloud.[258] However, toll records only provided other phone numbers with which the phone user, Mills, exchanged calls or text messages and not the content of the calls or messages. The iCloud data in Mills' case was significant, but her phone had stopped backing up data on iCloud several months prior to the incident, so the available information was stale for investigators.[259] Investigators were never able to access Mills' encrypted phone on their own despite seeking assistance from federal agencies.[260] Finally, after two years of investigating Mills' murder, police were able to access her phone after Cellebrite, a forensic software company, was able to get into the device.[261] Mills' killer, however, remains at large.

[254] Manhattan District Attorney's Office, 5.

[255] Manhattan District Attorney's Office, 5.

[256] Arrti Shahani, "Mom Asks: Who Will Unlock Murdered Daughter's IPhone?," NPR, March 30, 2016, https://www.npr.org/sections/alltechconsidered/2016/03/30/472302719/mom-asks-who-will-unlock-her-murdered-daughters-iphone.

[257] Shahani.

[258] Shahani.

[259] Shahani.

[260] Shahani.

[261] Grace Toohey, "Two Years Later, Brittney Mills Murder Case Still Unsolved after DA Hired Private Company to Crack IPhone," *The Advocate*, May 8, 2017, https://www.theadvocate.com/baton_rouge/news/crime_police/article_cb662d0a-2f74-11e7-ae45-5b4734c52601.html.

4. Mass Shootings: Dayton, OH (2019) and Southerland Springs, TX (2017)

Like Mills' killing, many high-profile attacks in the United States have not provided important closure for families of victims. One such incident occurred on August 4, 2019 when a 24-year-old man named Connor Betts, donning body armor, approached a bar in an entertainment district in Dayton, OH in the early morning hours with a rifle and high-capacity magazines.[262] Betts managed to fire 41 rounds in 30 seconds before local police killed him.[263] He killed nine people in the shooting, including his sister.[264] An examination of Betts' publicly available social media postings revealed no specific motive for the shooting, although it did reveal an interest in violence.[265] In addition, he reportedly kept a list of people to kill and expressed an interest in violence in some papers police found at his home.[266] Betts also had once compiled a list of female students at his high school who he wanted to sexually assault, which led to his suspension from the school.[267]

Days after the shootings, the FBI told members of Congress that its agency could not unlock a cell phone that the FBI possessed and believed was Betts' primary cell phone.[268] The phone was protected by a passcode, according to the FBI, which could take months or years to access.[269] Investigators likely wanted to access the phone to determine whether Betts had any accomplices, as well as a motive for his actions.

[262] WLWT Digital Staff, "Police: Dayton Gunman Fired at Least 41 Shots in 30 Seconds, Killing 9," WLWT, August 6, 2019, https://www.wlwt.com/article/9-killed-at-least-16-hurt-in-shooting-in-daytons-oregon-district/28599430.

[263] WLWT Digital Staff.

[264] WLWT Digital Staff.

[265] Paul Murphy et al., "Dayton Shooter Had an Obsession with Violence and Mass Shootings, Police Say," CNN, August 7, 2019, https://www.cnn.com/2019/08/05/us/connor-betts-dayton-shooting-profile/index.html.

[266] Murphy et al.

[267] Michael Biesecker and Julie Carr Smyth, "Ohio Gunman's Ex-Classmates Decry Missed Chances to Stop Him," *Associated Press*, August 6, 2019, https://apnews.com/83e222c2be834d1fb3b472f9f77aabb2.

[268] Timothy R. Homan and Scott Wong, "FBI Tells Lawmakers It Can't Access Dayton Gunman's Phone," The Hill, August 8, 2019, https://thehill.com/homenews/administration/456742-fbi-tells-lawmakers-it-cant-access-phone-of-dayton-gunman.

[269] Homan and Wong.

In a similar incident, on November 5, 2017, Devin Patrick Kelley pulled out a rifle outside the First Baptist Church in Southerland Springs, TX.[270] He began firing, and then went inside during Sunday service and kept shooting.[271] After getting into a shootout outside the church with a local resident, Kelley fled in his car and committed suicide in the adjacent county.[272] Kelley killed 23 at the church in a case that drew attention for several reasons, including a prior court-martial for Kelley when he was in the Air Force. It became notable because the Air Force had failed to enter the punishment into the National Crime Information Center database, which would have excluded Kelley from being able to purchase a gun.[273]

What also brought attention to Kelley's case were the two cell phones found in his car. One of Kelley's phones was an older, non-smartphone style phone. The other device was a blood-covered iPhone.[274] In a news conference two days after the shooting, the FBI announced that it did not have the ability to access Kelley's iPhone because it was locked.[275] The day before this announcement from the FBI, Texas Rangers obtained a search warrant for the phone that was in the FBI's possession at the time of the news conference.[276]

In the application supporting that warrant request, a Texas Ranger provided several reasons why the data on the phone would be important to his investigation. The reasons are specific to this case but layout why many criminal investigations into terroristic acts like Kelley's are often dependent on evidence gleaned from mobile devices. Among the items cited by the applicant documenting the need for the search warrant were that suspects often

[270] Jason Hanna and Holly Yan, "Sutherland Springs Church Shooting: What We Know," CNN, November 7, 2017, https://www.cnn.com/2017/11/05/us/texas-church-shooting-what-we-know/index.html.

[271] Hanna and Yan.

[272] Hanna and Yan.

[273] Hanna and Yan.

[274] "Read the Warrants Issued in Sutherland Springs Shooting Probe," *San Antonio Express-News*, November 20, 2017, https://www.expressnews.com/news/local/article/Read-the-warrants-issued-in-Sutherland-Springs-12371911.php.

[275] "FBI Having Difficulty Unlocking Texas Shooter Devin Kelley's Cellphone," November 7, 2017, NBC News, video, 1:15, https://www.youtube.com/watch?v=Ko_Jk-eFnRQ.

[276] "Read the Warrants Issued in Sutherland Springs Shooting Probe."

use their smartphones to communicate through various means and often do so with other criminals, suspects often memorialize their crimes with photos and other media, and suspects often use their phones to investigate methods to commit and hide evidence of their acts.[277] Another important part of the Ranger's application that supports law enforcement's need to access Kelley's phone, and in reality many phones that law enforcement seeks to search, is that data on a phone often documents a "timeline of events," as well as the presence and identification of witnesses or other suspects involved in the crime.[278] This Ranger's application explains why access to locked and encrypted devices like Kelley's and Betts' phones are so vital to terror investigations.

5. The Commonalities

The U.S. Attorney General, in the press conference for Alshamrani's case, and the Texas Rangers in their application to search Kelley's iPhone both highlighted perhaps one of the most pressing reasons why law enforcement seeks to access mobile devices following terror attacks and mass shootings, the need to determine whether the attacker communicated with anyone else about the attack. Such information could have significant implications for an investigation, including bringing any co-conspirators to justice. Even more pressing, such information may reveal further attack planning by actors associated with the attacker by either group membership or motive, or common direction by an organization like the Islamic State as demonstrated by the activities of Junaid Hussain.

Other law enforcement agencies around the country have cited the need to access locked devices. In the Manhattan DA's 2019 report on encryption, the office indicates that an examination of a locked device, specifically citing Betts' phone as an example, is vital because it provides "immediate evidence of his [the offender's] motives, other victims, other pending dangers, and unknown accomplices."[279] For a local agency like the Manhattan DA, the kind of evidence that could be recovered could lead to the rescue of

[277] "Read the Warrants Issued in Sutherland Springs Shooting Probe."

[278] "Read the Warrants Issued in Sutherland Springs Shooting Probe."

[279] Manhattan District Attorney's Office, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: October 2019*, 4.

victims of human trafficking and child sexual exploitation. It could mean locating accomplices actively committing crimes and harming people. It could be the difference between the acquittal of a possibly dangerous person and the conviction of someone who would continue to harm if left unchecked.

C. THE HYPOTHETICAL

The aforementioned cases aim to demonstrate the need for access to encrypted data by law enforcement and intelligence agencies. They further demonstrate how the trend of increased encryption is hampering security services' ability to detect, disrupt, and investigate nefarious acts, and rescue or protect victims or potential victims. This thesis now analyzes the various alternatives that have been proposed or suggested by many in the academic, technology, and legal investigative fields. To do so, a more detailed case study is helpful. The following case study sets out to foster the analysis. Although hypothetical, details of this scenario have been adapted from an actual investigation conducted by a local-level police department in the United States.

On June 13, at one o'clock in the afternoon, a municipal police agency receives a report to the city's tip line of child sexual abuse involving an infant male victim. The person reporting the incident does not leave a name. The tip indicates that a person named Maryann Smith is sexually assaulting her infant son, John, in her residence at the behest of her boyfriend. Smith exclusively communicates with her boyfriend through the FaceTime feature on her iPhone. The tipper does not report any information about the boyfriend.

Through open source searching, city detectives locate a Maryann Smith living in the city who is 25-years old. Two detectives obtain her address from her current driver's license and find her at her home at eight o'clock that night with her son, John, and her mother. She agrees to go the police station for an interview. John remains with his grandmother. Detectives drive Maryann to the police station. She brings her smartphone.

At the police station, Maryann is shown to a small room with a small table and three chairs. After several minutes, two detectives read Maryann her Miranda rights and she agrees to answer the detectives' questions. Maryann admits that she sexually assaulted her infant son about eight times. Every time she did so was during a video session with her boyfriend. Maryann relates that her boyfriend directs her to commit various acts on her infant while he watches. On three occasions, the boyfriend appeared in the chat with his 5-year-old son who was also forced to commit sexual acts by the boyfriend. Maryann tells detectives that her boyfriend discusses forcing the boy, John, to perform sexual acts on a regular basis.[280]

Maryann claims she met her boyfriend online but refuses to provide the specific website. Maryann tells detectives that she only knows his first name, Brad, and believes he lives one state away. She has never met him in person. Detectives seize her phone and apply for a search warrant for the device to identify the boyfriend, locate and rescue the second child victim, and develop enough evidence to arrest the boyfriend. Detectives ask but Maryann refuses to provide her smartphone passcode. She tells detectives that her boyfriend instructed her to delete any cloud backup of the phone's data regularly. She refuses to reveal the application she uses to communicate with him.

A city judge signs a warrant granting the police the right to search the phone based on an affidavit of one of the detectives. Despite a four-month backlog, the police department's computer forensics unit immediately attempts to access the phone citing the need to locate the second victim as soon as possible. The city's forensics unit is state of the art and has the best-trained personnel and the best equipment. The unit can access several kinds of devices with Android and iPhone operating systems that feature default full-disk encryption. However, the unit quickly realizes it is not equipped to access this device. The tools and equipment that allow the unit to essentially break into encrypted devices, which the unit purchases from private companies, do not support the operating system on Maryann's phone. The unit decides to hold the device in its lab in the hope that one of the companies will develop software that can hack into Maryann's phone. Since police cannot access Maryann's phone, they have no other sources of potential evidence. They are at a dead-end in trying to locate the second child victim and arrest the perpetrator.

[280] Details about these acts have been withheld because of the graphic nature of the acts that occurred.

D. CONCLUSION

Each of these case studies, when examined individually, illustrates why government agencies' access to digital data, the kind rendered inaccessible by end-to-end, full-disk, or file-based encryption, is an important element that determines the success or failure of an investigation. The hypothetical matter provides granular detail for detailed analysis because such information is usually not readily available in circumstances in which a perpetrator is not identified or charged. When the case studies are examined cumulatively, they substantiate the arguments made by many that lawful access by law enforcement and the IC is needed for both public safety and homeland security reasons. Digital evidence and the content of communications provide crucial information to investigators and intelligence analysts that can lead to disrupting attacks, rescuing victims, stopping offenders, and exonerating the innocent.

Computer scientists and scholars have introduced alternatives to providing lawful access to encrypted systems for government agencies. The same cases introduced in this chapter also assist in analyzing the alternatives presented in the next chapter; the alternatives are examined to determine their viability as policy options for law enforcement and the IC.

IV. ANALYSIS OF ALTERNATIVES TO LAWFUL ACCESS

The case studies in Chapter III demonstrate the need that law enforcement and the IC have for lawful access to encrypted data. The other stakeholders in this debate, however, maintain the position that strong encryption, with no allowance for lawful access, is the only appropriate policy. Technology companies, cryptographers, computer scientists, and privacy advocates are among these stakeholders. Their position is borne out of a legitimate concern that nefarious actors at some point will exploit some type of mandated access and thus compromise the security and privacy that users expect from their devices and applications.

Many of the stakeholders have countered the government's claim to need mandated lawful access by proposing or outlining alternatives. These alternatives fit generally into two categories. The first are alternatives that allow the government access to the content it seeks with search warrants and wiretap orders, such as via lawful hacking and compelled passcode disclosure, but do not require a mandate requiring government access. The second category is made up of alternatives in which the government uses different data sources, alternative information as a substitute, that experts argue is adequate to serve the needs of law enforcement and intelligence agencies to include metadata and cloud storage.

This chapter explores the most common alternatives and analyzes those alternatives, using the case studies and hypothetical scenario presented in Chapter III as a reference point, to draw conclusions as to the viability of the alternatives as policy options in the United States. The alternatives analyzed as follows appear in the literature about this debate. They have been proposed or advocated by computer science and technology experts, scholars, attorneys, and others who have expertise in at least some elements of the debate. This analysis relies on the four criteria delineated in Chapter I in determining their respective viability as policy alternatives to the lawful access challenge. The four criteria are as follows:

- The policy solution preserves law enforcement's ability to develop evidence needed to prosecute criminals and terrorists.

- The policy solution protects civil rights and civil liberties.
- The policy solution preserves the United States' national security and public safety.
- The government's implementation of the policy solution is feasible.

A. LAWFUL HACKING

No agreed-upon definition of what is referred to as lawful hacking exists. When referenced in the context of encryption, or more specifically, the going dark debate, the term is often applied as describing a means of intercepting encrypted communications.[281] For others, the term applies to the exploitation of flaws in software that is used to access plaintext data on encrypted devices and in encrypted messaging applications.[282] The term has also been applied to accessing encrypted data housed in cloud storage.[283] Cloud storage maintains digital files on servers usually owned by a hosting company. It is relevant to this debate because many use cloud storage to backup files on mobile devices. Law enforcement does not use any comparable terminology for the term lawful hacking.

1. The Approach

Lawful hacking, in general, is a concept in which law enforcement agencies exploit software vulnerabilities, operating within predetermined legal boundaries, with the intent of accessing encrypted data. Variations are available within the literature but this definition encapsulates the intent behind the approach. Computer science scholars in "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" discuss the lawful hacking approach in the context of encrypted messaging. "Lawful Hacking" describes a system in which law enforcement acts like nefarious actors and takes advantage of security

[281] Bellovin et al., "Lawful Hacking," 3–6.

[282] Lewis, Zheng, and Carter, *Effect of Encryption on Lawful Access to Communications and Data*, 26–28.

[283] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate,* 72.

holes in software programs to access decrypted data.[284] The same principal is applied to the lawful hacking of devices with full-disk or file-based encryption in that vulnerabilities are exploited to gain access to a device without the user's passcode.[285] This approach has been described as a "middle-ground solution" and one that is politically acceptable in that it does not require a mandate that would be perceived as weakening privacy standards.[286]

Implementation of lawful hacking as policy has led to concern on legal, ethical, and technical fronts. One recurring ethical issue is whether the government has an obligation to inform technology companies of the vulnerabilities that enable access to data on their systems.[287] If the government reports the vulnerability, the company responsible is likely to issue a patch making that vulnerability unavailable for further exploitation.[288] Another concern is the implications for the security of a system if a nefarious actor is able to gain access to and exploit a vulnerability that a government agency is using in accordance with a lawful hacking policy.[289] An important observation is that this concern is synonymous to the primary reason why so many oppose lawful access to encrypted data; which is that a nefarious actor will be able to exploit the same access point in furtherance of some type of malign scheme.[290] Further, lawful hacking may not be a solution for local law enforcement, a contingent that makes up the majority of law enforcement agencies.[291] Highly sensitive vulnerabilities may require the intense use of resources and technical skills or abilities that state and local law enforcement may not have.[292] A small number of third-

[284] Bellovin et al., "Lawful Hacking," 5.

[285] Lewis, Zheng, and Carter, *Effect of Encryption on Lawful Access to Communications and Data*, 7.

[286] Nguyen, "Lawful Hacking," 66–68.

[287] Olivia Gonzalez, "Cracks in the Armor: Legal Approaches to Encryption," *University of Illinois Journal of Law, Technology & Policy* 2019, no. 1 (2019): 30–31, http://illinoisjltp.com/journal/wp-content/uploads/2019/05/Gonzalez.pdf.

[288] Riana Pfefferkorn, *Security Risks of Government Hacking* (Palo Alto, CA: The Center for Internet and Society, 2018), 3, http://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf.

[289] Bellovin et al., "Lawful Hacking," 48.

[290] Pfefferkorn, *Security Risks of Government Hacking*, 9–10.

[291] Alan Rozenshtein, "Wicked Crypto," *UC Irvine Law Review* 9, no. 5 (July 1, 2019): 1207–8.

[292] Rozenshtein, 1207–8.

party companies currently offer services, including software-based products that can assist law enforcement in accessing at least some encrypted devices. Nonetheless, lawful hacking is offered as a policy solution to the lawful access challenge.

2. The Analysis

Lawful hacking does not represent an adequate policy solution to the lawful access challenge. Independent of the points raised by scholars regarding some of the potential ethical concerns, practical concerns are also raised with this approach as it relates to implementing it in terrorism and criminal investigations. One concern with lawful hacking is the timeliness of accessing the device, especially in situations in which an immediate risk to public safety may exist. In both the Pensacola and San Bernardino shooting events described in Chapter III, the attackers' devices were accessed, but not for several months after the attacks. Therefore, if any of the devices contained evidence of any co-conspirators, additional attack plans, or important homeland security or public safety intelligence, all of which is plausible, this information would have been hidden when it was needed the most. While there is no indication the FBI has publicly disclosed what was found on the San Bernardino phone, the Pensacola shooter's phone did contain important information about the shooter's association with an Al Qaeda member who was acted upon by the CIA.[293] Although lawful hacking techniques worked in both these cases, that such a technique took months to work is not a reasonable solution for the preservation of either U.S. public safety or homeland security.

Several months after the FBI accessed the San Bernardino phone, reports surfaced that FBI leadership was not "forthright" with Congress over the agency's ability to access the phone following the shooting.[294] If true, this statement would refute the conclusion that lawful hacking was not a solution in that case. However, such a claim is inaccurate. It is based on a DOJ Inspector General (IG) report of an inquiry into concerns of FBI

[293] Williams, "FBI" (as previously noted).

[294] Nate Cardozo and Andrew Crocker, "The FBI Could Have Gotten into the San Bernardino Shooter's IPhone, but Leadership Didn't Say That," Electronic Frontier Foundation, April 2, 2018, https://www.eff.org/deeplinks/2018/04/fbi-could-have-gotten-san-bernardino-shooters-iphone-leadership-didnt-say.

leadership that units in the agency may have been able to access the phone when the FBI director had testified that they did not.[295] The report found that the FBI had no ability to access the phone but was also not proactive enough in "researching all possible solutions."[296] The IG determined a resultant delay in getting help from a vendor.[297] However, the FBI challenged this conclusion and argued that the vendor was already working on a solution at the time of the shooting, and it had been a priority for the vendor for a while.[298] Nonetheless, no technical solution was available at the time that would have allowed law enforcement to access the phone when it needed the access the most.

In regards to another concern, the usefulness lawful hacking has in intercepting encrypted messages sent via communication applications falls short also. Rashaad Aubrey Smith's case illustrates this issue as it relates to the problem of child pornography transmitted over the internet. NCMEC has already highlighted this issue publicly noting that not even service providers are able to intercept this material when end-to-end decryption is deployed.[299] Had Smith been using a more secure product, such as Surespot used by Junaid Hussain in communicating with Abdulkader and Elton Simpson in his communications with an ISIS recruiter prior to his attack in Garland, TX, NCMEC likely would have never learned about the child pornography Smith received over the internet. End-to-end encryption ensures that even Surespot cannot see the content of the messages transmitted by its own users. These case studies illustrate the challenges that reliance on lawful hacking pose in developing evidence needed for criminal prosecutions.

Lawful hacking as a policy solution is also not workable because of the detrimental effect such a policy would have on smaller state and local law enforcement agencies.

[295] Office of the Inspector General, *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an IPhone Seized during the San Bernardino Terror Attack Investigation* (Washington, DC: Department of Justice, 2018), 1, https://oig.justice.gov/reports/2018/o1803.pdf.

[296] Office of the Inspector General, 9.

[297] Office of the Inspector General, 9.

[298] Office of the Inspector General, 10.

[299] National Center for Missing and Exploited Children, "NCMEC's Statement Regarding End-to-End Encryption."

Smaller agencies simply do not have the resources, in terms of equipment, training, and personnel, to be able to use lawful hacking to access encrypted data. Further, the technology that law enforcement relies on to access encrypted devices is expensive and does not include the added cost of the forensic hardware and software needed to conduct such digital forensics. While federal agencies may be able to assist with training and equipment deficiencies, the burden of devoting personnel can still be too great for many agencies.[300]

In the hypothetical scenario introduced in Chapter III, the subject device is never accessed because the police do not have the capability to do so, which leaves the investigation at a dead end. The agency may be able to seek the assistance of a larger, better-resourced agency but such resources may not be readily apparent to an investigator unfamiliar with lawful hacking techniques.[301] This scenario demonstrates that, consequently, small agencies end up being affected by encryption more so than ones with larger payrolls, more equipment, and heftier budgets.[302] Lawful hacking does not work for them. Without the resources of a large agency, lawful hacking may never be a workable solution for all 18,000 state and local law enforcement agencies, which makes its implementation infeasible for U.S. law enforcement.

This situation exists because technology companies have positioned themselves as, what scholar Alan Z. Rozenshtein calls, “surveillance intermediaries.”[303] The term refers to the large technology companies that “constrain” government surveillance; in essence, putting up road blocks to keep the government from accessing their customers’ data.[304] Companies do so for a variety of reasons, and not necessarily, to hinder the government,

[300] “National Computer Forensics Institute,” National Computer Forensics Institute, accessed July 19, 2020, https://www.ncfi.usss.gov/ncfi/index.xhtml?dswid=-8755.

[301] Anne Boustead, “Small Towns, Big Companies: How Surveillance Intermediaries Affect Small and Midsize Law Enforcement Agencies,” *Hoover Institution*, Aegis Series, 16, February 7, 2018, https://www.hoover.org/research/small-towns-big-companies.

[302] Boustead, 1.

[303] Alan Z. Rozenshtein, “Surveillance Intermediaries,” *Stanford Law Review* 70, no. 1 (2018): 105, https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/01/70-Stan.-L.-Rev.-99.pdf.

[304] Rozenshtein, 105.

although Rozenshtein posits that anti-surveillance ideology does play a role.[305] Thus, is the intent to be more competitive in the marketplace, particularly the foreign markets where Snowden's disclosures made many of these companies' foreign customers suspect of the United States' surveillance activities.[306]

While the premise that lawful hacking is infeasible for small agencies because of the likely lack of necessary resources, it should not be construed that larger agencies are able to devote resources to as potentially large an undertaking as lawful hacking. The discussion of lawful hacking often includes a recommendation, or at least, acknowledgement that such an undertaking will require an increase in resources for law enforcement. Such recommendations or acknowledgements have included creating an FBI laboratory to assist local agencies with lawful hacking expertise and federal law enforcement assuming particular types of investigations from state and local agencies.[307] Both would be major endeavors for federal agencies. It should be a concern for the feasibility of this alternative that, if implemented, the lawful hacking proposal will call for the obligation of significant assets. In addition, Lewis, Zheng, and Carter identify another complication involving resources, an "arms race dynamic" may develop as the technology companies continuously seek out ways to ensure their products cannot be accessed through vulnerabilities that government agencies can try to exploit.[308]

Despite all its drawbacks, lawful hacking is the only alternative that comes closest to giving the government access to the data it legally seeks. Several of the case studies indicate that law enforcement uses intrusive techniques to access decrypted data with no assistance from hardware or software makers. Law enforcement eventually accessed the Pensacola, San Bernardino, and Mills phones. However, assurances that law enforcement will be able to continue to access devices does not currently exist today and may never exist. Kerr and Schneier acknowledge this point in "Encryption Workarounds" and say that

[305] Rozenshtein, 118–19.

[306] Rozenshtein, 117–18.

[307] Nguyen, "Lawful Hacking," 76; Kerr and Schneier, "Encryption Workarounds," 10.

[308] Lewis, Zheng, and Carter, *Effect of Encryption on Lawful Access to Communications and Data*, 27.

the “uncertainty is inherent.”[309] If lawful hacking were adopted as the primary policy toward dealing with encryption, law enforcement could eventually be shut out of all mobile devices.

In addition, lawful hacking proposals often include an element of legal requirements, such as minimization procedures, vulnerability reporting requirements, and adherence to Fourth Amendment requirements.[310] In fact, legal aspects of access proposals are already a part of law enforcement actions in this realm since police are encountering encryption in instances in which search warrants and wiretap orders have been obtained and certain minimization procedures are already an element of executing wiretap orders. While overly burdensome legal requirements risk making lawful hacking financially or logistically unfeasible for agencies, reasonable additional requirements may be a significant contributor to ensuring the lawful hacking alternative preserves the civil rights and civil liberties of all involved.

B. METADATA

Metadata is information that provides knowledge about items, files, other data, etc.[311] Metadata can be of multiple different types, such as descriptive, administrative, and use metadata.[312] Descriptive metadata is information that describes an item. Administrative metadata is data about the creation and continuation of an item and is sometimes defined further as including structural or preservation metadata.[313] Use metadata is data about how an item has been used.[314] Metadata can contain a variety of information to include phone numbers someone has called, the location of a smartphone,

[309] Kerr and Schneier, “Encryption Workarounds,” 10.

[310] Nguyen, “Lawful Hacking,” 75–76.

[311] Jeffrey Pomerantz, *Metadata* (Cambridge: MIT Press, 2015), 26–27, ProQuest.

[312] Pomerantz, 17–18.

[313] Pomerantz, 17–18.

[314] Pomerantz, 17–18.

and the destinations of text communications like emails.[315] Metadata has become integral, even "infrastructural," in the information technology of everyday life.[316]

Metadata has historically been associated with library cataloguing, but it came into prominence with the Snowden revelations including those about the collection of metadata by intelligence agencies.[317] The amount of metadata available to law enforcement and intelligence agencies has been rising due to the proliferation of technologies that use and generate metadata.[318] Metadata is often accessible to law enforcement and intelligence agencies because it is often unencrypted even when it is descriptive of encrypted data.[319]

1. The Approach

The approach of using metadata as an alternative to lawful access to encrypted data is a simple one. Instead of using the contents of a file containing communications or other digital evidence, law enforcement relies on unencrypted metadata as the evidence instead. This approach is often discussed in tandem with the notion that government agencies have entered a "golden age of surveillance," an age in which the world's security agencies have access to vast amounts of data that can be used for investigative purposes.[320] One of those sources is metadata.

Metadata does have significant value to law enforcement because it furnishes useful evidence that can identify suspects and victims and even provide their locations.[321] It often proves useful in criminal investigations and can be compelling evidence. In 2011, for

[315] Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance* (New York: Henry Holt and Company, 2014), chap. 2.

[316] Pomerantz, *Metadata*, 3.

[317] Pomerantz, 1–6.

[318] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate*, 1–2.

[319] National Academies of Sciences, Engineering and Medicine, 39.

[320] Peter Swire and Kenesa Ahmad, "'Going Dark' versus a 'Golden Age for Surveillance,'" *Center for Democracy and Technology*, November 8, 2011, https://cdt.org/insights/'going-dark'-versus-a-'golden-age-for-surveillance'/.

[321] Lewis, Zheng, and Carter, *Effect of Encryption on Lawful Access to Communications and Data*, 25.

example, police arrested four subjects for armed robbery in Michigan.[322] After one of the subjects implicated several other individuals in the robberies, the FBI sought location data, a type of metadata, related to a cellular telephone owned by someone named Timothy Carpenter.[323] The metadata implicated Carpenter in the robberies since it showed that he, or at least his device, was in the general vicinity of the robberies when they occurred.[324] Often, police can use such metadata to find video surveillance to corroborate their findings. The U.S. Supreme Court eventually heard Carpenter's case when he challenged the way in which the FBI obtained his data.[325] This challenge led to a ruling by the court that law enforcement must obtain a search warrant to obtain such information from a telecommunications company.[326]

Metadata is similarly useful in the intelligence realm, often for the same reasons. It can provide valuable information that can help IC agencies locate adversaries, establish timelines, verify statements by sources, etc. In 2019, Bellingcat, a group of investigative journalists who utilize open-source intelligence techniques in their reporting, analyzed the cellular telephone metadata of a high-ranking member of Russia's military intelligence agency, often abbreviated as GRU.[327] Bellingcat had previously identified the officer as Denis Sergeev although his cell phone was registered in the name of an alias, Sergey Fedotov.[328] Bellingcat exploited the intelligence officer's telephone metadata to determine that he was in London, United Kingdom at the same time that two GRU operatives were also in the city.[329] The UK police charged the two operatives for poisoning Sergey Skripal,

[322] *United States v. Timothy Ivory Carpenter*, No. 14–1572, 2 (6th Cir. 2016), https://www.opn.ca6.uscourts.gov/opinions.pdf/16a0089p-06.pdf.

[323] *Carpenter*, No. 14–1572 at 2–3.

[324] *Carpenter*, No. 14–1572 at 2–3.

[325] Sabrina McCubbin, "Summary: The Supreme Court Rules in Carpenter v. United States," *Lawfare* (blog), June 22, 2018, https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states.

[326] McCubbin.

[327] Bellingcat Investigative Team, "The GRU Globetrotters: Mission London," Bellingcat, June 28, 2019, https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/.

[328] Bellingcat Investigative Team.

[329] Bellingcat Investigative Team.

a former GRU officer and double agent for the British, and his daughter.[330] Bellingcat was able to track the intelligence officer's movements so precisely that it could determine when he left the airport for the city center and even certain elements of his route.[331] Bellingcat's findings from the metadata analysis that have intelligence value include Sergeev's movements and presence in London during Skripal's poisoning and insight into the GRU's covert operating procedures when outside Russia.[332]

2. The Analysis

One reason for not relying on metadata in place of accessing encrypted data is that metadata does not contain the important invaluable content and vital evidence in both law enforcement investigations and intelligence analysis. While it has been proven that metadata has significant value to police and intelligence agencies, the need to access the content of communications and files cannot be replaced by metadata alone in many instances. In several of the case studies in Chapter III, authorities relied on content, not metadata, in the furtherance of their investigations or intelligence activities, which demonstrated the importance communications content holds in ensuring homeland security and public safety. Information derived from the contents of written or verbal communications can be the central factor in achieving a favorable outcome in a law enforcement investigation or intelligence operation. Content contains details about someone's intent, plotting activities, incriminating images or videos, and other important evidence not contained in metadata. Access to content has been crucial in preventing terrorist attacks and prosecuting criminals.

Several of the case studies in Chapter III illustrate the value of content in achieving this goal. Namouh was arrested after the content of his communications that indicated he was planning an attack were intercepted.[333] Similarly, in Zazi's case, an attack was

[330] Bellingcat Investigative Team.

[331] Bellingcat Investigative Team.

[332] Bellingcat Investigative Team.

[333] United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, 86–88 (as previously noted).

prevented because Zazi was found to be in the planning phase of multiple attacks based on the content of his communications.[334] Hussain and Abdulkader illustrate the contrasting situation when only metadata can be analyzed instead of content. Luckily, Abdulkader's attack was foiled because of the involvement of an informant who provided the content. However, had Abdulkader not given the informant the information he did, it is unlikely counterterrorism investigators would have been able to learn all the details of Abdulkader's plot. Metadata may have revealed that Abdulkader and Hussain were communicating, but only the content of the communications would have revealed the target of the attack, the method for conducting it, and the timing. It is possible that investigators would have been able to derive some intelligence from cell phone location data or financial records, but that would also depend on Abdulkader carrying his cell phone at all times, which he might not have done to avoid detection. Metadata cannot replace the value of content in assuring public safety and successfully prosecuting defendants for their crimes. In other words, the use of metadata fails to satisfy two of the criteria used by this thesis in judging its effectiveness as a viable alternative.

Metadata has proven to be useful as an investigative tool by law enforcement, and the *Carpenter* case helps illustrate that usefulness. Notwithstanding *Carpenter's* requirement that a search warrant is needed to obtain location metadata from a third-party service provider, metadata has been something that law enforcement agencies across the world have sought for years to aid in criminal investigations.[335] Whether Americans' civil rights and civil liberties are adequately protected by this alternative to encryption access is less clear. Collection of metadata by the government has attracted much more scrutiny since the Snowden disclosures and revelation of bulk collection practices by the NSA. Snowden believes such collection was a violation of the data owners' constitutional rights; however, the Supreme Court has ruled that the Fourth Amendment does not guard data

[334] Pantucci, "Manchester, New York and Oslo," 10–12 (as previously noted).

[335] Alastair MacGibbon, "Access to Metadata Is Vital for Crime Fighting: Says Internet Safety Advocate," *Sydney Morning Herald*, January 30, 2015, https://www.smh.com.au/technology/access-to-metadata-is-vital-for-crime-fighting-says-internet-safety-advocate-20150130-1322uw.html.

held by a third party.[336] In other words, courts have determined that information like dialed phone numbers, credit card information, etc., can be turned over to the government.[337]

The ruling in *Carpenter* was related specifically to location information on the user's cell phone that the court viewed as providing an "intimate window" into the device user's life that constituted a search thus requiring a warrant.[338] Going forward, *Carpenter* may have implications for law enforcement's access to metadata held in private hands that may provide similar details into someone's private life.[339]

C. COMPELLED DISCLOSURE

For many years, accessing a mobile device required only turning on the device. Any person could pick up a device and access everything on it, which for years amounted to little information held on the device but dialed and received calls and contact lists. Now, users secure their devices, and only users, or those to whom the users have provided the means of access, hold the information necessary to access those devices. In contrast to the two previous approaches, compelled disclosure is primarily a discussion of legal issues, rather than technical ones.[340]

1. The Approach

The approach of compelling disclosure is relatively simple, and as the name implies, is the concept of requiring disclosure of access information from device users. This approach generally, and usually, in the context of devices featuring file-based and full-disk encryption, involves two methods of accessing a device, biometric identifiers like

[336] Timothy Geverd, "Bulk Telephony Metadata Collection and the Fourth Amendment: The Case for Revisiting the Third-Party Disclosure Doctrine in the Digital Age," *The John Marshall Journal of Information Technology & Privacy Law* 31, no. 2 (2014): 192–93.

[337] Geverd, 192–93.

[338] McCubbin, "Summary."

[339] Paul Ohm, "The Many Revolutions of Carpenter," *Harvard Journal of Law & Technology* 32, no. 2 (Spring 2019): 359.

[340] Kerr and Schneier, "Encryption Workarounds," 7.

fingerprints and facial scans or passcodes.[341] This approach has been introduced as a method that would necessitate a court order that would come with the threat of contempt if a person refused to comply.[342]

2. The Analysis

The most significant criticism of compelled disclosure as an alternative to lawful access is that it cannot be implemented in situations in which the device user is not present. It has been noted that it not only applies to the death of the device user, as illustrated in several of the case studies, but also in situations during which the user cannot be found or may be in a country that does not cooperate with the U.S. government in law enforcement investigations.[343] Several of the case studies affirm this criticism since many of the device users either died in an attack, such as in the Pensacola, San Bernardino, Dayton, and Southerland Springs shootings, or died as a victim of a crime, such as with the murder of Brittany Mills.

In addition to the issue of the presence of the user, important legal ramifications must be considered when discussing this approach as an alternative to lawful access, as it has implications on the device owners' constitutional rights. These ramifications are rooted in the U.S. Constitution's Fifth Amendment right that no one can be compelled to be a witness against oneself.[344] It has been noted that much of the legal debate in the literature is corroborated by court decisions. It must be realized, however, that the U.S. Supreme Court has not weighed in on compelled access to a passcode yet. An important aspect of this debate centers on the use of "the contents of his own mind" when answering to the production of documents, or more specifically, encrypted data.[345] The issue in the decision from *In Re Grand Jury Subpoena Duces Tecum* at the U.S. Court of Appeals for the

[341] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate*, 50–52.

[342] Gasser et al., *Don't Panic*, Appendix A, 2.

[343] Kerr and Schneier, "Encryption Workarounds," 6.

[344] U.S. Constitution, amend. 5.

[345] *In Re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011 (USA v. John Doe),* 670 F.3d 1335, 20 (11th Cir. 2012), http://media.ca11.uscourts.gov/opinions/pub/files/201112268.pdf.

Eleventh Circuit, which centered on access to hard drives, is whether someone is required to "communicate some statement of fact" has played a large role in courts' decisions on compelling subjects to unlock their smartphones.[346] Thus, the legal debate centers more on the ability to compel subjects to enter their passcodes, which this thesis views as similar to compelling disclosure since both provide the desired outcome, or that of access to a locked device.

Currently, a debate is focused on the application of the Fifth Amendment to compelled passcode disclosure, which leaves the impact of the compelled disclosure alternative unsettled for now. Kerr has written extensively on this issue. He concludes that a subject can be compelled to provide a passcode if prosecutors or investigators can show that the subject knows the device's passcode.[347] Kerr argues that courts should not rule so that the law favors technology over society's need for law enforcement to be able to accomplish its crime-fighting mission.[348] While Kerr's arguments indicate that the constitutional concerns are less significant, lower court rulings have agreed and disagreed with Kerr. Kerr acknowledges that court cases on this topic are "all over the map."[349]

Court rulings have diverged on the subject of the application of the Fifth Amendment to compelled disclosure of a passcode, with no decisions involving the specific question from the Supreme Court. The Eleventh Circuit addressed this issue in *In Re Grand Jury Subpoena Duces Tecum* when it ruled that subjects cannot be compelled to disclose a passcode since decrypting the contents is testimonial as the subject is revealing contents of their minds, which results in the "communic(ation) of fact" as referenced earlier.[350] The Eleventh Circuit reviewed two U.S. Supreme Court cases relevant to the concept of compelled passcode disclosure as a whole. In *U.S. v. Hubbell*, a decision that occurred well

[346] *In Re: Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 at 20.

[347] Orin S. Kerr, "Compelled Decryption and the Privilege against Self-Incrimination," *Texas Law Review* 97, no. 4 (September 12, 2018): 769–70, https://papers.ssrn.com/abstract=3248286.

[348] Kerr, 770.

[349] Orin S. Kerr, "Decryption Originalism: The Lessons of Burr," *Harvard Law Review (Forthcoming)*, 2, February 6, 2020, https://papers.ssrn.com/abstract=3533069.

[350] *In Re: Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 at 20.

before encrypted smartphones, the Court found that a subject cannot be compelled to produce documents for which the government has not been able to demonstrate it is specifically aware of because that is akin to compelling the person to testify about the incriminating documents.[351] In *Fisher v. U.S.*, the Supreme Court decided that a subject could be compelled to produce documents that the government knew to exist, thus making the existence of the documents a "foregone conclusion in that situation." The Fifth Amendment was not applicable since the production of the documents was not a testament that they existed.[352]

State courts have also heard cases on the issue of compelled production of a passcode, but have diverged in their rulings. In Massachusetts, in the case *Commonwealth vs. Dennis Jones*, the court concluded that the foregone conclusion doctrine applied and the defendant must enter his passcode to decrypt access to his device for examination by law enforcement since the state was able to provide "clear and convincing evidence" that Jones knew the passcode.[353] The court also noted that the prosecution must prove beyond a reasonable doubt that a subject knows a passcode for the doctrine to apply in compelled disclosure cases.[354] Similarly, in *State v. Johnson*, a Missouri appellate court heard an appeal from a defendant who was compelled to enter his passcode that he was seen to enter into his phone for his defense team while also in the presence of a police officer.[355] The appeal to suppress evidence subsequently found on his device on the basis that the court wrongly violated his Fifth Amendment privilege by compelling disclosure was denied. The appellate court determined that it was a forgone conclusion that the defendant knew his passcode because he had entered it into his phone in front of the officer.[356] The court also noted in its decision that compelling the passcode was not a violation of the Fifth

[351] *United States v. Webster L. Hubbell*, 530 S. Ct. 27, 8–14 (2000).

[352] *John Vile, Fisher v. United States* (1976), No. 74–18, 411 (U.S. 1976).

[353] *Commonwealth vs. Dennis Jones*, No. SJC-12564, 4–19 (Mass. 2019), https://cases.justia.com/massachusetts/supreme-court/2019-sjc-12564.pdf?ts=1551964421.

[354] *Jones*, No. SJC-12564 at 12.

[355] *State v. Johnson*, No. WD80945, 16–17 (Mo. Ct. App. 2019), https://cases.justia.com/missouri/court-of-appeals/2019-wd80945.pdf?ts=1551804689.

[356] *Johnson*, No. WD80945 at 33–36.

Amendment in this case simply because incriminating evidence was discovered on the device after it was opened.[357] These state courts have determined that a subject can be compelled to unlock a device by disclosing the passcode when the government can prove the subject has knowledge of the passcode, which thereby satisfies the foregone conclusion doctrine.

However, other courts have ruled differently on the issue. In Illinois, the state's appellate court ruled in *People v. Spicer* that the analysis should center on the contents of the device, not the passcode itself.[358] The court determined in a narcotics possession case that even if the subject's knowledge of the passcode is a foregone conclusion, the issue at hand is whether to permit access to the documents on the device.[359] Thus, the court determined that in an order to compel disclosure of the passcode to access the phone, the government must be able to identify with some particularity the documents it seeks.[360] In this case, the prosecution only surmised that incriminating information was located on the smartphone because of the nature of the crime and the role cell phones often play in its commission.[361] An Indiana Supreme Court ruling also found in favor of a stricter view of a subject's rights involving compelled disclosure that enables decryption when it decided in 2020 that subjects cannot be compelled to unlock their devices unless the government articulates that the documents it seeks are on the device.[362] In the decision, the court advised that when suspects surrender passcodes, these suspects are implicitly testifying that they possess the data on the device, thereby giving the government knowledge it did not have, in opposition to the intention of the Fifth Amendment.[363] Kerr notes that this Indiana

[357] *State v. Johnson*, No. WD80945 at 35–36.

[358] *People v. Spicer*, No. 3–17–0814, 5 (Ill. App. Ct. 2019), https://courts.illinois.gov/Opinions/AppellateCourt/2019/3rdDistrict/3170814.pdf.

[359] *Spicer*, No. 3–17–0814 at 5.

[360] *Spicer*, No. 3–17–0814 at 5.

[361] *Spicer*, No. 3–17–0814 at 5–6.

[362] *Katelin Eunjoo Seo v. State of Indiana*, No. 18S-CR-595, 9 (Ind. 2020), https://www.in.gov/judiciary/opinions/pdf/06232001lhr.pdf.

[363] *State of Indiana*, No. 18S-CR-595 at 9.

Supreme Court ruling could lead to the U.S. Supreme Court taking up this issue since it is a clear split with Massachusetts' high court's *Jones* decision.[364]

Legal scholar Laurent Sacharoff has written in opposition to Kerr's views on this issue. He has aligned with the Indiana court's decision. Sacharoff notes that the government can compel disclosure of a passcode if it first has evidence to indicate a subject knows that certain files are on a device and the government is able to describe them with some particularity.[365] Sacharoff argues that Kerr's reliance on the foregone conclusion doctrine is erroneous because it is a "faulty premise."[366] It is faulty because the act of unlocking a device with a passcode is communicating more than just knowledge of the passcode; it also communicates the knowledge of the contents on the device.[367] The disagreement between Kerr and Sacharoff is analogous to the disagreements between the various courts. The outcome of any future decisions is thus murky and leaves the status of constitutional rights unclear as it pertains to the compelled disclosure alternative.

Legal hurdles aside, the compelled disclosure alternative suffers from other potential drawbacks, a person providing an incorrect passcode, a person's refusal to comply, or a person's claim the code has been forgotten. A defendant refusing to produce a passcode may be hiding evidence of crimes even beyond which the defendant has been charged. More importantly is the motivation of the defendant and that defendant's tolerance of a penalty for being found in contempt of court rather than for the potential exposure of more heinous crimes because of the evidence contained on a device. Penalties for contempt depend on the type of contempt the act is, criminal or civil.[368] Failing to obey the order of a court to disclose a passcode would be categorized as civil contempt. Whereas the penalty

[364] Orin Kerr, "Indiana Supreme Court Creates a Clear Split on Compelled Decryption and the Fifth Amendment," *Reason*, June 24, 2020, https://reason.com/2020/06/24/indiana-supreme-court-creates-a-clear-split-on-compelled-decryption-and-the-fifth-amendment/.

[365] Laurent Sacharoff, "What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr," *Texas Law Review* 97 (April 4, 2019): 64, https://texaslawreview.org/wp-content/uploads/2019/04/Sacharoff-TLRO-V97.pdf.

[366] Sacharoff, 64.

[367] Sacharoff, 68–69.

[368] "Contempt of Court," Legal Information Institute, May 2020, https://www.law.cornell.edu/wex/contempt_of_court.

for criminal contempt is definite, relief from penalty for civil contempt is generally conditional on the defendant complying with the court's order.[369]

In the hypothetical situation provided in Chapter III, if a court ordered Smith to disclose her passcode, she may refuse for reasons, such as protecting the identity of her boyfriend or fear of discovering evidence of further criminal activity. If Smith chooses to weigh a penalty of confinement for contempt versus one for a more serious charge, she may very well choose to accept confinement for contempt. In 2015, a subject of a criminal investigation into child pornography was confined for civil contempt after he failed to comply with a court order to provide passwords for two hard drives.[370] The subject, a former Philadelphia police officer named Francis Rawls, never disclosed the passwords and was eventually released after approximately five years.[371] Rawls was released after he appealed his confinement, which resulted in a ruling by the U.S. Court of Appeals for the Third Circuit that confinement for contempt should not exceed 18 months.[372] Considering the much lengthier sentences for the crimes potentially faced by Smith, refusing to comply with a compelled disclosure order could result in a much lighter sentence, and thus weaken the notion of compelled disclosure as a viable option in place of lawful access.

Compelled disclosure as an alternative to lawful access has many hurdles for effective implementation, especially when examined using the criteria set forth in this thesis. The case studies and uncertain Fifth Amendment legal issues referenced previously demonstrate the difficulty this alternative may have in ensuring public safety and criminal prosecution since device users must be present and alive to be able to provide a passcode, assuming they can be compelled. This issue is important for civil rights and civil liberties as well since future court decisions may continue to hamper compelled decryption as a legal alternative.

[369] Legal Information Institute.

[370] *United States v. Apple MacPro Computer et al.*, No. 17–3205 (3d Cir. 2020).

[371] Jeremy Roebuck, "Ex-Philadelphia Cop Freed after Years without Charges in Child Porn Probe," *Philadelphia Inquirer*, February 8, 2020, https://www.inquirer.com/news/ex-philadelphia-police-sergeant-freed-child-porn-francis-rawls-20200208.html.

[372] *Apple MacPro Computer et al.* at 15.

D. THE CLOUD

The final alternative analyzed by this thesis, obtaining data from a device's backup in cloud storage, appears less frequently in the literature compared to the previously described alternatives. The cloud, or more specifically cloud computing, is a variety of hardware and software services that provide users with accessible, off-site infrastructure available on a pay for use basis.[373] For many organizations, cloud computing represents an alternative method of obtaining and maintaining information technology to the organization's own information technology systems.[374]

1. The Approach

Cloud computing is generally categorized as providing three types of service: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).[375] SaaS offers reliable software and hardware services, such as e-mail, which is managed by a third-party vendor.[376] PaaS is a service that offers an entire platform, such as an operating system, to a client who can then run a variety of applications.[377] IaaS provides features similar to PaaS but without much of the services of maintaining information technology resources, and thus, is akin to a "leased infrastructure."[378] Many telecommunications companies offer data storage services in the cloud, such as Apple's iCloud service, which is basically an SaaS product.[379] Telecommunications companies like Apple and Verizon offer these cloud storage services

[373] Rajkumar Buyya, James Broberg, and Andrzej Goscinski, eds., *Cloud Computing*, 1st ed. (Hoboken, NJ: John Wiley & Sons, Ltd, 2011), 4–5, https://doi.org/10.1002/9780470940105.

[374] Grace Lewis, *Cloud Computing Basics Explained* (Pittsburgh: Software Engineering Institute, 2010), 1, https://resources.sei.cmu.edu/asset_files/WhitePaper/2010_019_001_28877.pdf.

[375] Suryanarayana Srinivasan, *Cloud Computing Basics* (New York: Springer, 2014), 17–19, https://doi.org/10.1007/978-1-4614-7699-3.

[376] Srinivasan, 19.

[377] Srinivasan, 24.

[378] Srinivasan, 26.

[379] Hitesh Patel, "Apple's iCloud: Why Should We Care?," IBM, July 18, 2011, https://www.ibm.com/blogs/cloud-computing/2011/07/18/apples-icloud-why-should-we-care/.

specifically to allow device users to back up the data held on their device in the event that the device is lost.[380]

Cloud storage services usually require the user affirmatively to obtain and pay for the service with pricing generally based on the amount of storage sought. iPhone users, for example, receive five gigabytes of data free from Apple, Inc. before Apple requires a paid subscription for further storage capacity.[381] Users of Apple products may choose to subscribe for access of up to two terabytes per month.[382] Verizon Cloud offers cloud storage for mobile devices and computers for up to two terabytes for a monthly fee but no free options currently exist.[383] Google offers 15 gigabytes free with Google Drive, and increased storage is available for cost through the company's Google One cloud service.[384] Thus, only a limited amount of a device's data, if any at all, may be in cloud storage unless a device user has subscribed to a cloud storage service.

Cloud storage backups are often not encrypted, which means law enforcement can access the device's backup data in the cloud when a device is impenetrable because of full-disk or file-based encryption, if the device user has chosen to utilize such a service.[385] In fact, reports surfaced in early 2020 that Apple retreated from plans to install encryption for data stored on iCloud after U.S. law enforcement requested Apple not do so out of concern for the effects on criminal investigations.[386] Law enforcement can thus obtain a search warrant for the data held in a device's cloud backup and access that data, when such a backup exists. In circumstances in which a device is impenetrable because of encryption

[380] "iCloud," Apple, accessed August 8, 2020, https://www.apple.com/icloud/; "Verizon Cloud—Mobile Phone Backup," Verizon, accessed August 8, 2020, https://www.verizon.com/solutions-and-services/verizon-cloud/.

[381] Apple.

[382] Apple.

[383] Verizon, "Verizon Cloud."

[384] "Google One," Google, accessed August 16, 2020, https://one.google.com/about#upgrade.

[385] Kerr and Schneier, "Encryption Workarounds," 9–10.

[386] Joseph Menn, "Exclusive: Apple Dropped Plan for Encrypting Backups after FBI Complained–Sources," *Reuters*, January 21, 2020, https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT.

or the device is not in the government's possession, this backup and access can be a useful and fruitful means of accessing digital evidence believed to be held on the device.

Numerous challenges exist regarding the recovery of digital evidence from the cloud. The National Institute of Standards and Technology (NIST) has identified 65 challenges associated with extracting digital evidence from the cloud.[387] While these challenges relate to cloud computing as a whole, many are pertinent to recovering device backups from cloud storage, including dependence on third-party providers to recover needed evidence that may be hindered by things like a lack of resources.[388] Nonetheless, cloud storage is important to law enforcement and intelligence agencies since it can provide access to data when a device is unavailable, including inaccessible devices with impenetrable file-based or full-disk encryption.[389]

2. The Analysis

Despite its usefulness to law enforcement, exploiting cloud storage backups as an alternative to lawful access is not adequate in preserving the ability to prosecute criminals and terrorists well or maintain national security and public safety. The case studies demonstrate the limits of using cloud data in criminal and counterterrorism investigations. Before Cellebrite accessed Brittany Mills' phone, police were able to obtain files from a cloud backup.[390] However, her device had stopped backing files up several months prior, which left investigators without the most recent information until Cellebrite was able to access the phone nearly two years later.[391] Why Mills' device stopped backing up her files has not been disclosed; however, the need for device users to be paid subscribers to a cloud storage service like iCloud or Verizon Cloud suggests a limited pool of device users have

[387] National Institute of Standards and Technology, *NIST Cloud Computing Forensic Science Challenges*, NISTR 8006 (Draft) (Gaithersburg, MD: National Institute of Standards and Technology, 2014), 4, https://csrc.nist.gov/publications/detail/nistir/8006/draft.

[388] National Institute of Standards and Technology, 35.

[389] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate*, 38.

[390] Shahani, "Mom Asks."

[391] Shahani; Toohey, "Two Years Later, Brittney Mills Murder Case Still Unsolved after DA Hired Private Company to Crack IPhone."

complete backups of their devices in cloud storage. Farook's phone also had a backup in cloud storage; however, that backup was last updated six weeks prior to the San Bernardino attack, which meant that law enforcement could not access the phone's information about its activities in the weeks leading up to the attack.[392] In both Farook's and Mills' cases, third parties eventually accessed both devices, but neither was accessed in a helpful amount of time. The cloud backups that investigators were able to access both had gaps of the most recent, and likely crucial, data the phones held.

Additionally, device users can usually modify settings on a device to stop cloud storage or simply choose not to activate the paid service when their free limit is reached.[393] Some may actually hinder future evidence and intelligence gathering by simply disabling or not subscribing to cloud storage for their mobile devices, which makes cloud storage a poor alternative to mandating lawful access.

Exploiting cloud storage backups as an alternative to lawful access is not adequate in preserving the ability to prosecute criminals and terrorists or maintaining national security and public safety. First, the need for device users to be paid subscribers to a cloud storage service like iCloud or Verizon Cloud suggests that a limited pool of device users have complete backups of their devices in cloud storage. Further, despite the availability of free options for limited storage like iCloud's five or Google Drive's 15 gigabyte allowance, mobile device users can usually modify settings on a device to stop cloud storage of their device or simply choose not to activate it.[394] Nefarious actors could too easily hinder evidence and intelligence gathering by simply disabling or not subscribing to cloud storage for their mobile devices, which makes it a poor alternative to mandating lawful access.

[392] Ellen Nakashima and Mark Berman, "FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup," *Washington Post*, sec. National Security, February 20, 2016, https://www.washingtonpost.com/world/national-security/fbi-asked-san-bernardino-to-reset-the-password-for-shooters-phone-backup/2016/02/20/21fe9684-d800-11e5-be55-2cc3c1e4b76b_story.html.

[393] National Academies of Sciences, Engineering and Medicine, *Decrypting the Encryption Debate*, 71.

[394] National Academies of Sciences, Engineering and Medicine, 71.

The other important criteria for evaluating these alternatives, feasible implementation, and protecting civil rights and liberties, are adequate under the cloud storage alternative. Considering that law enforcement agencies have already been using this alternative in appropriate circumstances, including with Farook's and Mills', implementation has already been achieved. Further, such access to cloud devices generally requires some type of legal process, such as a subpoena, search warrant, or other court order depending on the data sought and in whose possession it is. Apple reports the requests it receives from law enforcement for information including access to iCloud data. It received in excess of 9,500 requests from governments in the United States in the first half of 2019.[395] There is no reason to believe that Americans' civil rights and civil liberties are not being respected during the pursuit of cloud data by the government.

Although the cloud storage alternative has favorable analysis regarding implementation and the protection of civil rights and civil liberties, it does not outweigh detrimental effects this limited alternative may have on criminal prosecutions and national security. Cloud storage provides much more limited access than is needed and what lawful access seeks to obtain. There is too little chance that investigators and intelligence analysts would be able to access all the information they would need to do their duties than cloud storage could provide.

E. CONCLUSION

While this thesis has examined the alternatives individually, some of the literature on the subject suggests that the alternatives should be viewed in unison. That is, policy going forward should maintain that all these alternatives should be implemented instead of just a singular option as the solution. Where one alternative is not successful, another may be. When lawful hacking does not result in accessing a device, for example, collecting metadata may provide investigators and prosecutors with the evidence they need to move forward. However, as the analysis and the case studies illustrate, these alternatives have

[395] "Transparency Report: United States of America," Apple, accessed August 16, 2020, https://www.apple.com/legal/transparency/us.html.

too many drawbacks even when grouped as a whole because none can ensure complete access to the content that law enforcement needs.

Another gauge of the effectiveness of these alternatives in totality is that government agencies are already using all the alternatives yet still sounding the alarm for lawful access because of the challenges it continually faces in decrypting data. While these options are offered as alternatives to lawful access, they already serve as methods for investigation and intelligence collection on a regular basis, and are often fruitful methods as well. However, the case studies illustrate that in many instances, these methods are ultimately ineffective at granting agencies the range of access to the content of communications and mobile devices that those agencies need.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

The 21st century has brought with it many technological advances that are continually increasing in their sophistication, and doing so quite rapidly. This thesis highlights two such advances, encrypted messaging applications and encrypted smartphones. These advances have left law enforcement and intelligence agencies often unable to access important evidence and intelligence, which hinders their public safety and homeland security missions. Even in situations in which an agency has obtained a court-approved search warrant or wiretap, modern-day encryption still leaves those agencies locked out, which creates the lawful access challenge.

Law enforcement executives have been vocal about the challenge for many years, and the issue is often featured in the media when high-profile incidents involving encrypted devices or communications occur. Law enforcement faces the access challenge when investigating terrorists, drug dealers, child pornographers, and many other types of criminals. Most participants in this debate, if not all, seem to agree that law enforcement's concerns are legitimate. The debate is not a disagreement about whether encryption is a problem for law enforcement and the IC, but about what should be done about the issue.

This debate is often framed as a binary argument between those who prioritize privacy, privacy advocates, technology companies, and computer scientists versus those who prioritize security, primarily security agencies. This debate is hardly binary and each stakeholder that participates has its own priorities for doing so. Technology companies seek to remain competitive and provide products sought in the marketplace. Privacy advocates like the EFF seek to defend against government interference into internet governance. Computer scientists fear that accommodating law enforcement's needs will compromise information security. Even among law enforcement and intelligence organizations, the argument can differ for why lawful access is sought. The Manhattan DA's office, for example, focuses almost entirely on mobile device encryption.[396]

[396] Manhattan District Attorney's Office, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: October 2019*, 2–3.

Intelligence agencies place emphasis on both accessing mobile devices and intercepting communications over messaging applications.[397]

Cryptographers and computer science scholars also have weighed in heavily on the encryption debate. A minority has proposed possible solutions where law enforcement can have the access it needs while maximizing the security inherent in the strong encryption systems against which agencies are coming up. Many more experts steadfastly maintain that decrypting data for law enforcement's consumption weakens encryption and puts the personal data of every user of encrypted messaging applications and smartphones at risk. They argue that cyber criminals, nation-state adversaries, or an unscrupulous government will inevitably exploit such access. Meanwhile, no agreed-upon solution has been offered.

Many experts who express concern about weakening encryption have offered alternatives that they believe can fulfill law enforcement and intelligence needs without mandating lawful access. These alternatives include lawful hacking, use of metadata, compelled passcode disclosure, and exploiting cloud data, and are methods that these experts argue provide adequate access to needed information to satisfy public safety and homeland security concerns. The alternatives maintain user privacy while filling in the gaps created by encryption, experts assert. Law enforcement agencies have other means to conduct investigations, they maintain, without the need to access content protected by encryption. Law enforcement, in contrast, has argued that such content is in fact important and the alternatives that encryption advocates promote are deficient.

This thesis evaluated those alternatives in the context of case studies of incidents in which investigations were boosted by access to communications or device data, as well as instances in which encryption encumbered significant investigations pertinent to public safety and homeland security. When counterterrorism authorities in Europe intercepted communications of Said Namouh, for example, the information developed from the intercepts disrupted a terror attack in Europe.[398] Similarly, when UK authorities

[397] Bonnie Mitchell et al., *Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation* (Washington, DC: DHS Office of Intelligence and Analysis, 2017), 4–5, https://www.odni.gov/files/PE/Documents/10---2017-AEP_Going-Dark.pdf.

[398] United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, 86–88.

intercepted the email communications of Abid Naseer in 2009, the intercepts helped disrupt both Naseer's actions, as well as those of U.S.-based plotter Najibullah Zazi.[399] In contrast, after encrypted messaging applications became widespread, ISIS recruiter Junaid Hussain began communicating through such an application with Munir Abdulkader who planned to kill a government employee.[400] Another ISIS member was also found to have communicated via an encrypted messaging application with Elton Simpson who later attempted an attack on an anti-Islam event in Texas in 2015.[401] Some mass shootings have also provided important examples that illustrate why access to locked cell phones is important. Chapter III discusses similar incidents in 2017 in Southerland Springs, TX and in 2019 in Dayton, OH that occurred in which the shooter's phones were recovered but inaccessible due to encryption, which left investigators with no ability to obtain potentially important evidence like the existence of other actors or targets.

While the focus of these case studies is the perpetrators, accomplices, and additional attacks, several of the case studies presented in Chapter III highlight the effect encrypted devices and communications have on victims of crimes. The issue of the relationship between child pornography and end-to-end encryption, for example, is an important one for the encryption debate. This relationship receives less attention than the one between encryption and terrorism, even though it is much more widespread.[402] This relationship also continues to worsen considering the continued growth of reports of child pornography by technology companies. As the proliferation of child pornography reports continue to expand, it will become more and more difficult to defend the sanctity of end-to-end encryption.[403]

It is in the context of these case studies that the alternatives offered by computer science and cryptography experts were evaluated for their viability as policy options in

[399] Pantucci, "Manchester, New York and Oslo," 10–12 (as previously noted).

[400] Hamid, "The British Hacker Who Became the Islamic State's Chief Terror Cybercoach," 34 (as previously noted).

[401] Cooper, "60 Minutes Investigates First ISIS-Claimed Attack in U.S. and What the FBI Knew."

[402] Hennessey, *The Elephant in the Room*, 1–3.

[403] Hennessey, 1–3.

place of mandated, lawful access. Lawful hacking, however, is unreliable in ensuring access and potentially prohibitive in cost and skill to enact by federal, state, and especially, local law enforcement. Metadata fails to provide information and intelligence that fulfills agencies' abilities in both law enforcement and intelligence to maintain public safety and homeland security. Compelled passcode disclosure risks violate American's constitutional rights and civil liberties. Accessing cloud data, like lawful hacking, provides unreliable results unlikely to ensure agencies' can fulfill their public safety and homeland security missions. Even grouping these alternatives as a collective approach still does not adequately replace lawful access.

A. RECOMMENDATIONS

This thesis does not claim to have an answer to the encryption debate that will satisfy all stakeholders. To date, no balanced solution has been offered that provides the desired outcomes. Nonetheless, this thesis offers some recommendations to shift momentum closer to a solution.

1. Include Victims of Crime in the Debate

The encryption debate includes several stakeholder groups, and this thesis has discussed their positions. However, one group not heard from are the victims of crimes in which encryption is an element, which can include victims of terrorist attacks, violent crimes, child exploitation, fraud, etc., and their families. NCMEC advocates for victims of child exploitation in the encryption debate.[404] However, the literature that dominates the debate gives little attention otherwise to the effects of encryption on victims. Any future policy considerations regarding encryption should take into account the views that crime victims and survivors have on the issue.

Time constraints prevented this thesis from researching possible methods in implementing this recommendation; however, NCMEC represents a potential model for both advocacy and research on behalf of victims affected by encryption. NCMEC engages

[404] National Center for Missing and Exploited Children, "NCMEC's Statement Regarding End-to-End Encryption."

the media and legislators on important issues affecting victims of child exploitation and has been vocal about the impact end-to-end encryption has on preventing child exploitation.[405] NCMEC's work also includes research focused on its priorities, which include lowering and deterring child exploitation that complements the organization's other goals related to recovering missing children.[406] Considering the impacts that encryption can have on the wider population, lessons can be learned from NCMEC in addressing the issue on behalf of victims.

2. Modernize CALEA

A common refrain heard in today's age is that the law cannot keep up with the rapid pace of technology and CALEA embodies that notion. CALEA requires certain telecommunications companies, but not messaging applications, to be capable of providing law enforcement access to communications, including when encrypted. CALEA should be examined for potential amendments that can align this law, which provides the most current technologies. The act was last amended in 2004 and excluded many forms of communications transmitted over the internet and well before default encryption became popular.[407] Technology has been rapidly developing new means of communication on the internet and CALEA is becoming more and more out-of-date. CALEA should be updated to address encryption technologies.

3. Dedicated Research to Closing the Gaps

The final recommendation is that more computer scientists and cryptographers should research the potential for technologies that can allow companies to provide for lawful access. A gap exists between what law enforcement needs and what technology can tolerate. Computer scientists and cryptographers who participate in the encryption debate should follow the lead of scientists like Savage who have researched and proposed methods

[405] "End-to-End Encryption: Ignoring Abuse Won't Stop It," National Center for Missing and Exploited Children, accessed September 2, 2020, https://www.missingkids.org/theissues/end-to-end-encryption#overview.

[406] "About Us," National Center for Missing and Exploited Children, accessed September 2, 2020, https://www.missingkids.org/footer/about.

[407] McCarthy, "Decoding the Encryption Debate," 20–21, (as previously noted).

to permit lawful access while minimizing security and mass surveillance risks.[408] Public safety and homeland security may benefit from the examination of a solution that provides for both lawful access while maximizing data security.

Similar research recommendations that focus on dedicating funding to look for ways to strengthen government abilities at lawful hacking are misguided in that they ultimately recommend spending possibly vast sums of public money in thwarting security measures developed by American companies. The companies themselves should be relied upon for the solutions. These companies know their technologies the best and are best equipped at determining how to comply with warrants and court orders seeking decrypted data.

B. CONCLUSION

This thesis seeks to contribute to the debate on encryption by providing an analysis of the alternatives that experts have presented as options for law enforcement and intelligence agencies to use for gathering evidence and information to fulfill their missions. This analysis was conducted in the context of case studies involving criminal and counterterrorism investigations in which nefarious actors sought to hurt, kill, abuse, or otherwise victimize innocent people. It is important to determine whether the alternatives can truly stand up to the public safety and homeland security needs of the United States.

This thesis finds that the alternatives are not viable options to replace lawful access to encrypted data, either on their own or in totality. Nonetheless, law enforcement and intelligence agencies will surely continue to exploit these alternatives as they have been. While all the alternatives have shortcomings, as the analysis has shown, lawful hacking will continue to be the primary option for seeking access to encrypted data. Agencies are likely to continue devoting resources to acquiring the equipment and products that produce the results they require, which lawful hacking does better than any other alternative.

[408] Savage, "Lawful Device Access without Mass Surveillance Risk," 1761; Steven Levy, "Can This System of Unlocking Phones Crack the Crypto War?," Wired, April 25, 2018, https://www.wired.com/story/crypto-war-clear-encryption/.

The encryption debate sees no signs of abating, as recent events like the Pensacola shooting and proposed legislation, like the EARN IT Act, trigger both sides of the debate to reassert their positions for and against government access. Despite disagreement, the sides of the debate seek to strengthen U.S. national and homeland security. No one group is anti-encryption. No one group is opposed to U.S. security and public safety. All make strong cases for why encryption is important. It is important for all participants in this debate to try to find a solution.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Diffie Whitfield, and John Gilmore et al. "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." *Journal of Cybersecurity* 1, no. 1 (July 7, 2015): 69–79. https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

———. *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*. Washington, DC: Center for Democracy and Technology, 2017. https://doi.org/10.7916/D8GM8F2W.

Ablon, Lillian, David Aitel, Sofia d'Antoine, Edward Doyle, Thomas Garwin, Daniel Guido, and Nicholas Rostow et al. *Going Dark: Implications of an Encrypted World*. New York: New York Center for Advanced Study in Terrorism at Colombia University, 2017. https://nsiteam.com/going-dark-implications-of-an-encrypted-world/.

Administrative Office of the United States Courts. "Wiretap Report 2018." Last updated December 31, 2018. http://www.uscourts.gov/statistics-reports/wiretap-report-2018.

———. "Wiretap Report 2019." Last updated December 31, 2019. http://www.uscourts.gov/statistics-reports/wiretap-report-2019.

———. *Wiretap Report 2010*. Washington, DC: Administrative Office of the United States Courts, 2011. https://www.uscourts.gov/statistics-reports/wiretap-report-2010.

Adrian Shahbaz and Allie Funk. *Freedom on the Net 2019: The Crisis of Social Media." Freedom on the Net*. Washington, DC: Freedom House, 2019. https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.

American Civil Liberties Union. "About the ACLU." Accessed June 7, 2019. https://www.aclu.org/about-aclu.

Angwin, Julia. Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance. New York: Henry Holt and Company, 2014.

Apple. "iCloud." Accessed August 8, 2020. https://www.apple.com/icloud/.

———. "Transparency Report: United States of America." Accessed August 16, 2020. https://www.apple.com/legal/transparency/us.html.

Apple, Inc. "Data Protection Overview." Accessed August 17, 2020. https://support.apple.com/guide/security/data-protection-overview-secf6276da8a/1/web/1.

———. “Passcodes.” Accessed August 17, 2020. https://support.apple.com/guide/security/passcodes-sec20230a10d/1/web/1.

———. “Touch ID, Face ID, Passcodes, and Passwords.” Accessed August 17, 2020. https://support.apple.com/guide/security/touch-id-face-id-passcodes-and-passwords-sec9479035f1/1/web/1.

Associated Press. “Chinese Cyberattack Hits Encrypted Messaging App Used by Hong Kong Protesters.” *New York Post*, June 13, 2019. https://nypost.com/2019/06/13/chinese-cyberattack-hits-encrypted-messaging-app-used-by-hong-kong-protestors/.

Baker, Stewart. “The EARN IT Act Raises Good Questions about End-to-End Encryption.” *Lawfare* (blog). February 11, 2020. https://www.lawfareblog.com/earn-it-act-raises-good-questions-about-end-end-encryption.

Barlow, John Perry. “A Plain Text on Crypto Policy.” Electronic Frontier Foundation, September 6, 1993. https://www.eff.org/pages/plain-text-crypto-policy.

Barr, William P. “Attorney General William P. Barr Announces the Findings of the Criminal Investigation into the December 2019 Shooting at Pensacola Naval Air Station.” Department of Justice, January 13, 2020. https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-findings-criminal-investigation-december-2019.

BBC News. “Australia Passes Encryption-Breaking Laws.” December 7, 2018. https://www.bbc.com/news/world-australia-46463029.

———. “Russia to Block Telegram over Encryption.” April 13, 2018. https://www.bbc.com/news/technology-43752337.

Bellingcat Investigative Team. “The GRU Globetrotters: Mission London.” Bellingcat, June 28, 2019. https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/.

Bellovin, Steven M., Matt Blaze, Sandy Clark, and Susan Landau. “Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet.” *Northwestern Journal of Technology and Intellectual Property* 12, no. 1 (2014): 1–64. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip.

Benner, Katie, and Adam Goldman. “F.B.I. Finds Links between Pensacola Gunman and Al Qaeda.” *New York Times*, May 18, 2020. https://www.nytimes.com/2020/05/18/us/politics/justice-department-al-qaeda-florida-naval-base-shooting.html.

Biesecker, Michael, and Julie Carr Smyth. “Ohio Gunman’s Ex-Classmates Decry Missed Chances to Stop Him.” *Associated Press*, August 6, 2019. https://apnews.com/83e222c2be834d1fb3b472f9f77aabb2.

Black, Tricia E. “Taking Account of the World as It Will Be: The Shifting Course of U.S. Encryption Policy.” *Federal Communications Law Journal* 53, no. 2 (2001): 289–314. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1271&context=fclj.

Blaze, Matt. “Protocol Failure in the Escrowed Encryption Standard.” In *CCS94: 2nd ACM Conference on Computer & Communications Security*, 59–67. New York: Association for Computing Machinery, 1994. https://doi.org/10.1145/191177.191193.

Bohannon, Mark. “The State of Encryption: How the Debate Has Shifted.” Opensource.com, June 13, 2018. https://opensource.com/article/18/6/listening-susan-landau.

Boustead, Anne. “Small Towns, Big Companies: How Surveillance Intermediaries Affect Small and Midsize Law Enforcement Agencies.” *Hoover Institution*, Aegis Series, February 7, 2018. https://www.hoover.org/research/small-towns-big-companies.

Braun, Michael. “Collier Deputy Arrested; Report Says Search at Home Finds 100 Instances of Child Porn.” *Fort Myers News-Press*, June 14, 2020. https://www.news-press.com/story/news/crime/2020/06/14/collier-county-deputy-facing-100-counts-child-pornography/3187134001/.

Buyya, Rajkumar, James Broberg, and Andrzej Goscinski, eds. *Cloud Computing*. 1st ed. Hoboken, NJ: John Wiley & Sons, Ltd, 2011. https://doi.org/10.1002/9780470940105.

Cardozo, Nate, and Andrew Crocker. “The FBI Could Have Gotten into the San Bernardino Shooter’s IPhone, but Leadership Didn’t Say That.” Electronic Frontier Foundation, April 2, 2018. https://www.eff.org/deeplinks/2018/04/fbi-could-have-gotten-san-bernardino-shooters-iphone-leadership-didnt-say.

Carlile, Alex. *Operation Pathway: Report Following Review*. London: Independent Reviewer of Terrorism Legislation, 2009. https://webarchive.nationalarchives.gov.uk/20100416131809/http://security.homeoffice.gov.uk/news-publications/publication-search/legislation/terrorism-act-2000/operation-pathway-report.

Central Intelligence Agency. “CIA Vision, Mission, Ethos & Challenges.” November 1, 2018. https://www.cia.gov/about-cia/cia-vision-mission-values.

Chicago Police Department. “Mission.” Accessed March 18, 2020. https://www.chicago.gov/content/city/en/depts/cpd/auto_generated/cpd_mission.html.

Clement, J. “Facebook Messenger—Statistics and Facts.” Statista, June 25, 2019. https://www.statista.com/topics/4625/facebook-messenger/.

———. “Mobile Messaging Users Worldwide 2018–2022.” Statista, October 8, 2019. https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/.

Cohen, William, Jane Reno, Jacob J. Lew, and William Daley. *Preserving America’s Privacy and Security in the Next Century: A Strategy for America in Cyberspace*. Washington, DC: The White House, 1999. https://fas.org/irp/news/1999/09/990916-crypto-wh.htm.

Comey, James. “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?.” Federal Bureau of Investigation, October 16, 2014. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Cook, Tim. “Customer Letter.” Apple, Inc., February 16, 2016. http://www.apple.com/customer-letter/.

Cooper, Anderson. “60 Minutes Investigates First ISIS-Claimed Attack in U.S. and What the FBI Knew.” 60 Minutes, March 26, 2017. https://www.cbsnews.com/news/terrorism-in-garland-texas-what-the-fbi-knew-before-the-2015-attack/.

CTIA. “2019 Annual Survey Highlights.” June 20, 2019. https://www.ctia.org/news/2019-annual-survey-highlights.

Dahl, Erik J. “The Plots that Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks against the United States.” *Studies in Conflict & Terrorism* 34, no. 8 (August 1, 2011): 621–48. https://doi.org/10.1080/1057610X.2011.582628.

Department of Justice. “Cincinnati-Area Man Pleads Guilty to Plot to Attack U.S. Government Officers.” July 7, 2016. https://www.justice.gov/opa/pr/cincinnati-area-man-pleads-guilty-plot-attack-us-government-officers.

———. “Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy.” October 10, 2017. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

———. “Najibullah Zazi Indicted for Conspiracy.” September 24, 2009. https://www.justice.gov/opa/pr/najibullah-zazi-indicted-conspiracy.

———. “Three Arrested in Ongoing Terror Investigation.” September 20, 2009. https://www.justice.gov/opa/pr/three-arrested-ongoing-terror-investigation.

DIGI. Submission to the Parliamentary Joint Committee on Intelligence and Security on the Telecommunications and Other Legislation Amendment (Assistance and Access Bill) 2018. Canberra, Australia: DIGI, 2018. https://digi.org.au/advocacy/.

Electronic Frontier Foundation. "About EFF." Accessed June 7, 2019. https://www.eff.org/about.

———. "Privacy." Accessed June 7, 2019. https://www.eff.org/issues/privacy.

Elinson, Zusha, and Dan Frosch. "San Bernardino Shooting: How the Carnage Unfolded: Witnesses Recount Horror, Suspense as Bursts of Gunfire Interrupted Office Party." *Wall Street Journal*, December 4, 2015.

Eng, James. "FBI Director: Encrypted Messages Stymied Probe of 'Draw Muhammad' Shooting." NBC News, December 9, 2015. https://www.nbcnews.com/tech/security/fbi-director-encrypted-messages-stymied-probe-garland-shooting-n477111.

Fazzini, Kate. "FBI Director Wray: I Strongly Share Barr's Concerns about Encrypted Devices and Messaging Platforms, Cites Sutherland Springs Apple Case." CNBC, July 25, 2019. https://www.cnbc.com/2019/07/25/fbi-director-wray-i-strongly-share-barrs-concerns-about-encryption.html.

Federal Bureau of Investigation. "Going Dark." March 5, 2020. https://web.archive.org/web/20200305041805/https://www.fbi.gov/services/operational-technology/going-dark.

———. "The Lawful Access Challenge." Accessed August 6, 2020. https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch/lawful-access.

Federal Communications Commission. "OMB Approves CALEA Compliance Monitoring Report for Providers of Facilities-Based Broadband Internet Access and Interconnected VOIP Service; Reports Are Due February 12, 2007." December 14, 2006. https://www.fcc.gov/document/omb-approves-calea-compliance-monitoring-report-providers-facilities.

Feiner, Lauren. "AG Barr Says Tech Companies Need to Make Encrypted Messages Accessible to Law Enforcement." CNBC, July 23, 2019. https://www.cnbc.com/2019/07/23/bill-barr-tells-tech-to-open-encrypted-messages-for-investigations.html.

Finklea, Kristin M. *Encryption and the 'Going Dark' Debate*. CRS Report No. R44481. Washington, DC: Congressional Research Service, 2017. https://crsreports.congress.gov/product/details?prodcode=R44481.

Gasser, Urs, Matthew G. Olsen, Nancy Gertner, Daphna Renan, Jack Goldsmith, Julian Sanchez, and Susan Landau et al. *Don’t Panic: Making Progress on the ‘Going Dark’ Debate*. Cambridge, MA: Berkman Center for Internet & Society at Harvard Law School, 2016. https://dash.harvard.edu/bitstream/handle/1/28552576/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf?sequence=1&isAllowed=y.

Geverd, Timothy. “Bulk Telephony Metadata Collection and the Fourth Amendment: The Case for Revisiting the Third-Party Disclosure Doctrine in the Digital Age.” *The John Marshall Journal of Information Technology & Privacy Law* 31, no. 2 (2014): 191–236.

Gonzalez, Olivia. “Cracks in the Armor: Legal Approaches to Encryption.” *University of Illinois Journal of Law, Technology & Policy* 2019, no. 1 (2019): 1–48. http://illinoisjltp.com/journal/wp-content/uploads/2019/05/Gonzalez.pdf.

Google. “Google One.” Accessed August 16, 2020. https://one.google.com/about#upgrade.

Government Communications Headquarters. *Open Letter to GCHQ*. Cheltenham, United Kingdom: Government Communications Headquarters, 2019. https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf.

Greenberg, Andy. “Facebook Says Encrypting Messenger by Default Will Take Years.” Wired, January 10, 2020. https://www.wired.com/story/facebook-messenger-end-to-end-encryption-default/.

———. “Hacker Lexicon: What Is End-to-End Encryption?.” Wired, November 25, 2014. https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

Hamid, Nafees. “The British Hacker Who Became the Islamic State’s Chief Terror Cybercoach: A Profile of Junaid Hussain.” *CTC Sentinel* 11, no. 4 (April 26, 2018): 1–37. https://ctc.usma.edu/wp-content/uploads/2018/04/CTC-SENTINEL-042018-3.pdf.

Hanna, Jason, and Holly Yan. “Sutherland Springs Church Shooting: What We Know.” CNN, November 7, 2017. https://www.cnn.com/2017/11/05/us/texas-church-shooting-what-we-know/index.html.

Hennessey, Susan. *The Elephant in the Room: Addressing Child Exploitation and Going Dark*. Aegis Paper Series. Stanford, CA: Hoover Institution, Stanford University, 2017. https://www.hoover.org/sites/default/files/research/docs/hennessey_webreadypdf.pdf.

Hess, Amy. “Deciphering the Debate over Encryption.” Federal Bureau of Investigation, April 19, 2016. https://www.fbi.gov/news/testimony/deciphering-the-debate-over-encryption.

Homan, Timothy R., and Scott Wong. "FBI Tells Lawmakers It Can't Access Dayton Gunman's Phone." The Hill, August 8, 2019. https://thehill.com/homenews/administration/456742-fbi-tells-lawmakers-it-cant-access-phone-of-dayton-gunman.

House Committee on Homeland Security. *Going Dark, Going Forward: A Primer on the Encryption Debate*. Washington, DC: House Committee on Homeland Security, 2016. https://fas.org/irp/congress/2016_rpt/hsc-encrypt.pdf.

House Permanent Select Committee on Intelligence. *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden*. Washington, DC: U.S. Government Publishing Office, 2016. https://www.congress.gov/114/crpt/hrpt891/CRPT-114hrpt891.pdf.

Human Rights Watch. "Russia: 'Big Brother' Law Harms Security, Rights." July 12, 2016. https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

Jeschke, Rebecca. "Plan for Internet 'Backdoors' Draws Coordinated Attack." Electronic Frontier Foundation, October 26, 2005. https://www.eff.org/deeplinks/2005/10/plan-internet-backdoors-draws-coordinated-attack.

Joscelyn, Thomas. "AQAP Claims 'Full Responsibility' for Shooting at Naval Air Station Pensacola." *FDD's Long War Journal*, February 2, 2020. https://www.longwarjournal.org/archives/2020/02/aqap-claims-full-responsibility-for-shooting-at-naval-air-station-pensacola.php.

Kaul, Krystle, Michelle Tucker, G. S. McNamara, Jacqueline Hicks, Colin Bliss, Scott Tosi, and Lora Loethen. *Going Darker 2.0: Policy Recommendations for Law Enforcement, the Intelligence Community and the Private Sector*. Washington, DC: DHS Office of Intelligence and Analysis, 2018. https://www.dhs.gov/sites/default/files/publications/2018_AEP_Going_Darker_Phase2.pdf.

Kehl, Danielle, Andi Wilson, and Kevin Bankston. *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s*. Washington, DC: New America, 2015. https://static.newamerica.org/attachments/3407--125/Lessons%20From%20the%20Crypto%20Wars%20of%20the%201990s.882d6156dc194187a5fa51b14d55234f.pdf.

Keller, Michael H., and Gabriel J. X. Dance. "The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?." *New York Times*, September 29, 2019. https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

Kerr, Orin. "Indiana Supreme Court Creates a Clear Split on Compelled Decryption and the Fifth Amendment." *Reason,* June 24, 2020. https://reason.com/2020/06/24/indiana-supreme-court-creates-a-clear-split-on-compelled-decryption-and-the-fifth-amendment/.

Kerr, Orin S. “Compelled Decryption and the Privilege against Self-Incrimination.” *Texas Law Review* 97, no. 4 (September 12, 2018): 767–99. https://papers.ssrn.com/abstract=3248286.

———. “Decryption Originalism: The Lessons of Burr.” *Harvard Law Review (Forthcoming)*, February 6, 2020. https://papers.ssrn.com/abstract=3533069.

Kerr, Orin S., and Bruce Schneier. “Encryption Workarounds.” *Georgetown Law Journal* 106 (2017): 1–30. https://doi.org/10.2139/ssrn.2938033.

Khan Academy. “Encryption and Public Keys.” Accessed June 9, 2019. Video, 6:39. https://www.khanacademy.org/computing/computer-science/internet-intro/internet-works-intro/v/the-internet-encryption-and-public-keys.

Lee, Nicole. “Facebook Messenger Is Getting Faster, Lighter and More Secure in 2019.” *Engadget*, April 30, 2019. https://www.engadget.com/2019/04/30/facebook-messenger-f8-2019/.

Legal Information Institute. “Contempt of Court.” May 2020. https://www.law.cornell.edu/wex/contempt_of_court.

———. “Title 47 U.S. Code § 1002—Assistance Capability Requirements.” Accessed June 6, 2019. https://www.law.cornell.edu/uscode/text/47/1002.

Levy, Steven. “Can This System of Unlocking Phones Crack the Crypto War?.” Wired, April 25, 2018. https://www.wired.com/story/crypto-war-clear-encryption/.

Lewis, Grace. *Cloud Computing Basics Explained*. Pittsburgh: Software Engineering Institute, 2010. https://resources.sei.cmu.edu/asset_files/WhitePaper/2010_019_001_28877.pdf.

Lewis, James A., Denise E. Zheng, and William A. Carter. *The Effect of Encryption on Lawful Access to Communications and Data*. Washington, DC: Center for Strategic and International Studies, 2017. https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data.

Liao, Shannon. “Apple Officially Moves Its Chinese ICloud Operations and Encryption Keys to China.” *The Verge*, February 28, 2018. https://www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accounts-government-privacy-speed.

Los Angeles Police Department. “The Mission Statement of the LAPD.” Accessed March 18, 2020. http://www.lapdonline.org/inside_the_lapd/content_basic_view/844.

Los Angeles Times. “Timeline: The San Bernardino Shooting and Aftermath Step by Step.” December 6, 2015. https://www.latimes.com/visuals/graphics/la-g-san-bernardino-shooting-timeline-20151204-htmlstory.html.

MacGibbon, Alastair. “Access to Metadata Is Vital for Crime Fighting: Says Internet Safety Advocate.” *Sydney Morning Herald*, January 30, 2015. https://www.smh.com.au/technology/access-to-metadata-is-vital-for-crime-fighting-says-internet-safety-advocate-20150130-1322uw.html.

Manhattan District Attorney’s Office. “DA Vance: Babysitter Convicted at Trial for Sexually Assaulting Two Children.” November 28, 2017. https://www.manhattanda.org/da-vance-babysitter-convicted-trial-sexually-assaulting-two-children/.

———. *Report of the Manhattan District Attorney’s Office on Smartphone Encryption and Public Safety: October 2019*. New York: Manhattan District Attorney’s Office, 2019. https://www.manhattanda.org/wp-content/uploads/2019/10/2019-Report-on-Smartphone-Encryption-and-Public-Safety.pdf.

———. *Report of the Manhattan District Attorney’s Office on Smartphone Encryption and Public Safety: November 2018*. New York: Manhattan District Attorney’s Office, 2018. https://www.manhattanda.org/wp-content/uploads/2018/11/2018-Report-of-the-Manhattan-District-Attorney27s-Office-on-Smartphone-En....pdf.

Markoff, John. “Computer Code Plan Challenged.” *New York Times*, May 29, 1993. http://timesmachine.nytimes.com/timesmachine/1993/05/29/924093.html.

McCarthy, Hugh J. “Decoding the Encryption Debate: Why Legislating to Restrict Strong Encryption Will Not Resolve the ‘Going Dark’ Problem.” *Journal of Internet Law* 20, no. 3 (September 2016): 18–39. ProQuest.

McCubbin, Sabrina. “Summary: The Supreme Court Rules in Carpenter v. United States.” *Lawfare* (blog). June 22, 2018. https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states.

Meleagrou-Hitchens, Alexander, and Seamus Hughes. “The Threat to the United States from the Islamic State’s Virtual Entrepreneurs.” *Combating Terrorism Center at West Point* 10, no. 3 (March 9, 2017): 1–37. https://ctc.usma.edu/wp-content/uploads/2017/03/CTC-Sentinel_Vol10Iss331.pdf.

Menn, Joseph. “Exclusive: Apple Dropped Plan for Encrypting Backups after FBI Complained—Sources.” *Reuters*, January 21, 2020. https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT.

Miller, Joe. “Google and Apple Encrypt by Default.” BBC News, September 19, 2014. https://www.bbc.com/news/technology-29276955.

Mitchell, Bonnie, Krystle Kaul, G. S. McNamara, Michelle Tucker, Jacqueline Hicks, Colin Bliss, and Rhonda Ober et al. *Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation*. Washington, DC: DHS Office of Intelligence and Analysis, 2017. https://www.odni.gov/files/PE/Documents/10---2017-AEP_Going-Dark.pdf.

Motorola. "Data Encryption." Accessed June 6, 2019. https://support.motorola.com/in/en/solution/MS98572.

Murphy, Paul P., Konstantin Toropin, Drew Griffin, Scott Bronstein, and Eric Levenson. "Dayton Shooter Had an Obsession with Violence and Mass Shootings, Police Say." CNN, August 7, 2019. https://www.cnn.com/2019/08/05/us/connor-betts-dayton-shooting-profile/index.html.

Nakashima, Ellen, and Mark Berman. "FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup." *Washington Post*, February 20, 2016. https://www.washingtonpost.com/world/national-security/fbi-asked-san-bernardino-to-reset-the-password-for-shooters-phone-backup/2016/02/20/21fe9684-d800-11e5-be55-2cc3c1e4b76b_story.html.

National Academies of Sciences, Engineering and Medicine. *Decrypting the Encryption Debate: A Framework for Decision Makers*. Washington, DC: The National Academies Press, 2018. https://doi.org/10.17226/25010.

National Center for Missing and Exploited Children. "About Us." Accessed September 2, 2020. https://www.missingkids.org/footer/about.

———. "End-to-End Encryption: Ignoring Abuse Won't Stop It." Accessed September 2, 2020. https://www.missingkids.org/theissues/end-to-end-encryption#overview.

———. "NCMEC's Statement Regarding End-to-End Encryption." October 3, 2019. https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption.

National Computer Forensics Institute. "National Computer Forensics Institute." Accessed July 19, 2020. https://www.ncfi.usss.gov/ncfi/index.xhtml?dswid=-8755.

National Institute of Standards and Technology. *NIST Cloud Computing Forensic Science Challenges*. NISTR 8006 (Draft). Gaithersburg, MD: National Institute of Standards and Technology, 2014. https://csrc.nist.gov/publications/detail/nistir/8006/draft.

NBC News. "FBI Having Difficulty Unlocking Texas Shooter Devin Kelley's Cellphone." November 7, 2017. Video, 1:15. https://www.youtube.com/watch?v=Ko_Jk-eFnRQ.

New Jersey State Police. "Mission Statement." Accessed March 18, 2020. https://www.njsp.org/about/mission-statement.shtml.

Nguyen, Hoaithi Y. T. “Lawful Hacking: Toward a Middle-Ground Solution to the Going Dark Problem.” Master’s thesis, Naval Postgraduate School, 2017. http://hdl.handle.net/10945/53024.

O’Dea, S. “Mobile Operating Systems’ Market Share Worldwide from January 2012 to December 2019.” Statista, February 28, 2020. https://www.statista.com/statistics/ 272698/global-market-share-held-by-mobile-operating-systems-since-2009/.

———. “Smartphone Ownership Rate by Country 2018.” Statista, February 27, 2020. https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/.

Office of the Director of National Intelligence. “Mission.” Accessed March 15, 2020. https://www.intelligence.gov/mission.

Office of the Inspector General. A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an IPhone Seized during the San Bernardino Terror Attack Investigation. Washington, DC: Department of Justice, 2018. https://oig.justice.gov/reports/2018/o1803.pdf.

Ohm, Paul. “The Many Revolutions of Carpenter.” *Harvard Journal of Law & Technology* 32, no. 2 (Spring 2019): 358–415.

Pantucci, Raffaello. “Manchester, New York and Oslo.” *CTC Sentinel* 3, no. 8 (August 1, 2010): 1–28. https://ctc.usma.edu/wp-content/uploads/2010/10/CTCSentinel-Vol3Iss8-13.pdf.

Partz, Helen. “Russia May Lift Telegram Ban Due to Coronavirus Outbreak.” Cointelegraph, April 23, 2020. https://cointelegraph.com/news/russia-may-lift-telegram-ban-due-to-coronavirus-outbreak.

Patel, Hitesh. “Apple’s iCloud: Why Should We Care?.” IBM, July 18, 2011. https://www.ibm.com/blogs/cloud-computing/2011/07/18/apples-icloud-why-should-we-care/.

Patsakisa, Constantinos, Athanasios Charemis, Achilleas Papageorgiou, Dimitrios, Mermigas, and Sotirios Pirouniasa. “The Market’s Response toward Privacy and Mass Surveillance: The Snowden Aftermath.” *Elsevier* 73 (2018): 194–206. https://doi.org/10.1016/j.cose.2017.11.002.

PBS Newshour. “San Bernardino Press Conference with FBI.” December 7, 2015. Video, 15:09. https://www.pbs.org/newshour/nation/watch-live-san-bernardino-press-conference-with-fbi.

Pfefferkorn, Riana. *Security Risks of Government Hacking*. Palo Alto, CA: The Center for Internet and Society, 2018. http://cyberlaw.stanford.edu/files/publication/files/ 2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf.

———. “The EARN IT Act: How to Ban End-to-End Encryption without Actually Banning It.” *The Center for Internet and Society* (blog). January 30, 2020. http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it.

Pomerantz, Jeffrey. *Metadata*. Cambridge: MIT Press, 2015. ProQuest.

Roebuck, Jeremy. “Ex-Philadelphia Cop Freed after Years without Charges in Child Porn Probe.” *Philadelphia Inquirer,* February 8, 2020. https://www.inquirer.com/news/ex-philadelphia-police-sergeant-freed-child-porn-francis-rawls-20200208.html.

Roth, Andrew. “Russia Blocks Millions of IP Addresses in Battle against Telegram App.” *The Guardian*, April 17, 2018. https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app.

Rozenshtein, Alan. “Wicked Crypto.” *UC Irvine Law Review* 9, no. 5 (July 1, 2019): 1181–1216.

Rozenshtein, Alan Z. “Surveillance Intermediaries.” *Stanford Law Review* 70, no. 1 (2018): 99–189. https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/01/70-Stan.-L.-Rev.-99.pdf.

Sacharoff, Laurent. “What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr.” *Texas Law Review* 97 (April 4, 2019): 63–72. https://texaslawreview.org/wp-content/uploads/2019/04/Sacharoff-TLRO-V97.pdf.

San Antonio Express-News. “Read the Warrants Issued in Sutherland Springs Shooting Probe.” November 20, 2017. https://www.expressnews.com/news/local/article/Read-the-warrants-issued-in-Sutherland-Springs-12371911.php.

San Bernardino Sun. “Everything We Know about the San Bernardino Terror Attack Investigation.” November 27, 2016. https://www.sbsun.com/2016/11/27/everything-we-know-about-the-san-bernardino-terror-attack-investigation/.

Savage, Stefan. “Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion.” In *CCS ‘18: 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1761–1774. New York: Association for Computing Machinery, 2018. https://cseweb.ucsd.edu/~savage/papers/lawful.pdf.

Schneier, Bruce. “The EARN-IT Act.” *Schneier on Security* (blog). March 13, 2020. https://www.schneier.com/blog/archives/2020/03/the_earn-it_act.html.

Seigfried-Spellar, Kathryn C., Gary R. Bertoline, and Marcus K. Rogers. “Internet Child Pornography, U.S. Sentencing Guidelines, and the Role of Internet Service Providers.” In *Digital Forensics and Cyber Crime*, edited by Pavel Gladyshev and Marcus K. Rogers, 18–32. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. https://www.researchgate.net/publication/285975958_Internet_Child_Pornography_US_Sentencing_Guidelines_and_the_Role_of_Internet_Service_Providers.

Shahani, Arrti. “Mom Asks: Who Will Unlock Murdered Daughter’s IPhone?.” NPR, March 30, 2016. https://www.npr.org/sections/alltechconsidered/2016/03/30/472302719/mom-asks-who-will-unlock-her-murdered-daughters-iphone.

Shepherd, Todd. “Judge Dismisses Lawsuit Alleging FBI Role in 2015 Terror Attack in Texas.” *Washington Free Beacon*, January 5, 2019. https://freebeacon.com/issues/judge-dismisses-lawsuit-alleging-fbi-role-in-2015-terror-attack-in-texas/.

Simcox, Robin. *Surveillance after Snowden: Effective Espionage in an Age of Transparency*. London: The Henry Jackson Society, 2015. http://henryjacksonsociety.org/wp-content/uploads/2015/06/Surveillance-After-Snowden-16.6.15.pdf.

Spinello, Richard A. *Cyberethics: Morality and Law in Cyberspace*. 6th ed. Burlington, MA: Jones & Bartlett Learning, 2017.

Srinivasan, Suryanarayana. *Cloud Computing Basics*. New York: Springer, 2014. https://doi.org/10.1007/978-1-4614-7699-3.

Surespot. “How Surespot Works.” Accessed March 21, 2020. https://www.surespot.me/documents/how_surespot_works.html.

Swire, Peter, and Kenesa Ahmad. “‘Going Dark’ versus a ‘Golden Age for Surveillance.’” *Center for Democracy and Technology*, November 8, 2011. https://cdt.org/insights/’going-dark’-versus-a-’golden-age-for-surveillance’/.

Toohey, Grace. “Two Years Later, Brittney Mills Murder Case Still Unsolved after DA Hired Private Company to Crack IPhone.” *The Advocate*, May 8, 2017. https://www.theadvocate.com/baton_rouge/news/crime_police/article_cb662d0a-2f74-11e7-ae45-5b4734c52601.html.

U.S. Congress, House. Cyberspace Electronic Security Act of 1999--Message from the President of the United States, H. Doc. 106–123. 106th Cong., 1st sess. *Congressional Record* 145, no. 123 daily ed. (September 21, 1999): H8390–91. https://www.congress.gov/congressional-record/1999/9/21/house-section/article/H8390-8.

United Nations General Assembly. *The United Nations Global Counter-Terrorism Strategy*. New York: United Nations, 2006. https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy.

United Nations Office on Drugs and Crime. *The Use of the Internet for Terrorist Purposes*. Vienna: United Nations, 2012. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

United States House of Representatives Permanent Select Committee on Intelligence. "Intelligence Committee Ranking Member Schiff Statement on Encryption Debate in Wake of Paris Attacks." November 18, 2015. https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=196.

United States Secret Service. "The Protective Mission." Accessed August 17, 2020. https://www.secretservice.gov/protection/.

United States Senate Committee on the Judiciary. "Graham, Blumenthal, Hawley, Feinstein Introduce EARN IT Act to Encourage Tech Industry to Take Online Child Sexual Exploitation Seriously." March 5, 2020. https://www.judiciary.senate.gov/press/rep/releases/graham-blumenthal-hawley-feinstein-introduce-earn-it-act-to-encourage-tech-industry-to-take-online-child-sexual-exploitation-seriously.

ur Rehman, Ikhlaq. "Facebook-Cambridge Analytica Data Harvesting: What You Need to Know." *Library Philosophy and Practice*, 2019. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5833&context=libphilprac.

Vance, Cy. "Written Testimony for the United States Senate Committee on the Judiciary on Smartphone Encryption and Public Safety." Manhattan District Attorney's Office, December 10, 2019. https://www.manhattanda.org/written-testimony-for-the-united-states-senate-committee-on-the-judiciary-on-smartphone-encryption-and-public-safety/.

Verizon. "Verizon Cloud—Mobile Phone Backup." Accessed August 8, 2020. https://www.verizon.com/solutions-and-services/verizon-cloud/.

Volz, Dustin. "FBI Says No Misconduct in Inflated Number of Encrypted Phones." *Wall Street Journal*, May 23, 2018. https://www.wsj.com/articles/fbi-says-no-misconduct-in-inflated-number-of-encrypted-phones-1527113031.

Weise, Elizabeth. "Apple v FBI Timeline: 43 Days That Rocked Tech." *USA Today*, March 15, 2016. https://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400/.

Williams, Katie Bo. "Intelligence Community Pushes Back on Encryption Report." The Hill, May 9, 2016. https://thehill.com/policy/cybersecurity/279231-intelligence-community-pushes-back-on-pro-encryption-report.

Williams, Pete. "FBI: Pensacola Gunman Prodded by Al Qaeda to Attack." NBC News, May 18, 2020. https://www.nbcnews.com/news/us-news/fbi-pensacola-gunman-prodded-al-qaeda-attack-n1209276.

WLWT . “Police: Dayton Gunman Fired At Least 41 Shots in 30 Seconds, Killing 9.” August 6, 2019. https://www.wlwt.com/article/9-killed-at-least-16-hurt-in-shooting-in-daytons-oregon-district/28599430.

Wray, Christopher. “Finding a Way Forward on Lawful Access.” Federal Bureau of Investigation, October 4, 2019. https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California