NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LAWFUL HACKING: TOWARD A MIDDLE-GROUND SOLUTION TO THE GOING DARK PROBLEM

by

Hoaithi Y.T. Nguyen

March 2017

Thesis Co-Advisors: Carolyn Halladay
Ted Lewis

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** March 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE LAWFUL HACKING: TOWARD A MIDDLE-GROUND SOLUTION TO THE GOING DARK PROBLEM		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Hoaithi Y.T. Nguyen			
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. IRB number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

This thesis examines the ongoing debate between law enforcement and the intelligence communities on one side, and the technology industry and privacy rights groups on the other, over the "going dark" problem. Going dark is a phenomenon created by ubiquitous use of end-to-end encryption over communication devices and Internet platforms, rendering those communications warrant-proof. End-to-end encryption means that only the sender and receiver of the message can read it, and no one in between. Even with a properly executed warrant or subpoena, law enforcement and intelligence agencies are unable to access the data they need because that data was encrypted. This thesis explores the historical, political and legislative developments that contributed to the rise of encryption in recent years, as well as constitutional doctrines that may be relevant to the public debate over possible policy solutions. Through the policy options analysis method, this thesis identifies lawful hacking as a middle-ground solution that policymakers should adopt in the short term. It also recommends that the U.S. government initiate a public education campaign to gain public support for some form of regulation concerning encryption in the future. The fundamental issue here is not only about the tension between privacy and security. The issue is also about who should make decisions with broad implications for the collective security: elected officials or the technology industry.

14. SUBJECT TERMS going dark, end-to-end encryption, ubiquitous encryption, CALEA, lawful hacking, privacy versus security, liberty versus security, warrant proof communications, encryption code and the Fourth Amendment, encryption code and the First Amendment			**15. NUMBER OF PAGES** 105
			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

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

LAWFUL HACKING: TOWARD A MIDDLE-GROUND SOLUTION TO THE GOING DARK PROBLEM

Hoaithi Y.T. Nguyen
Attorney-Advisor, Office of Chief Counsel,
Transportation Security Administration
B.A., University of California, Irvine, 1992
J.D., University of California, Los Angeles, 1997

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
March 2017**

Approved by: Carolyn Halladay, Ph.D.
Thesis Co-Advisor

Ted Lewis, Ph.D.
Thesis Co-Advisor

Erik Dahl, Ph.D.
Associate Chair of Instruction, Department of Homeland Security

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines the ongoing debate between law enforcement and the intelligence communities on one side, and the technology industry and privacy rights groups on the other, over the "going dark" problem. Going dark is a phenomenon created by ubiquitous use of end-to-end encryption over communication devices and Internet platforms, rendering those communications warrant-proof. End-to-end encryption means that only the sender and receiver of the message can read it, and no one in between. Even with a properly executed warrant or subpoena, law enforcement and intelligence agencies are unable to access the data they need because that data was encrypted. This thesis explores the historical, political and legislative developments that contributed to the rise of encryption in recent years, as well as constitutional doctrines that may be relevant to the public debate over possible policy solutions. Through the policy options analysis method, this thesis identifies lawful hacking as a middle-ground solution that policymakers should adopt in the short term. It also recommends that the U.S. government initiate a public education campaign to gain public support for some form of regulation concerning encryption in the future. The fundamental issue here is not only about the tension between privacy and security. The issue is also about who should make decisions with broad implications for the collective security: elected officials or the technology industry.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
AES	Advanced Encryption Standard
AO	Administrative Office
CALEA	Communication Assistance to Law Enforcement Act
CCOA	Compliance with Court Order Act of 2016
CIPAV	Computer and Internal Protocol Address Verifier
DA	District Attorney
DES	Data Encryption Standard
DOJ	Department of Justice
EFF	Electronic Frontier Foundation
FBI	Federal Bureau of Investigation
FCC	Federal Communication Commission
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ISIL	Islamic State of Iraq in the Levant
ISIS	Islamic State of Iraq and ash-Sham
ISP	Internet Service Provider
ITAR	International Traffic in Arms Regulations
LEAF	Law Enforcement Access Field
MAC	media access control
NSA	National Security Agency
PKI	public-key infrastructure
SME	subject matter experts
URL	Uniform Resource Locator

USML	U.S. Munitions List
VEP	Vulnerability Equity Process
VoIP	Voice over Internet Protocol

EXECUTIVE SUMMARY

Since the spring of 2013, when Edward Snowden leaked classified information regarding the National Security Agency's (NSA) covert collection of telephony metadata from major communications providers, such Internet giants as Apple and Google have rolled out end-to-end encryption on their devices. End-to-end encryption means that "only the recipient of the message can decrypt it and not anyone in between."[1] Today, hundreds of millions of users of Apple iPhones, Google Chrome, Android, WhatsApp and many other Internet platforms and applications around the world are now enjoying end-to-end encryption. Indeed, a vast majority of technology providers have now designed the technology in such a way that they cannot access the data sought, even pursuant to a court order, because they do not hold the key.[2] The security situation is the same for data "at rest" on an electronic device or data "in motion" over electronic networks. This trend presents a unique challenge to law enforcement and intelligence communities. The hallmark of these agencies investigative tools is interception of communications that are now out of reach because of end-to-end encryption. This problem is known as the problem of "going dark."

The intelligence and law enforcement communities have been locked in a debate with privacy advocates and the technology industry over striking the right balance between individual liberty and collective security. The rhetoric on both sides of the debate has not served to find possible solutions despite the many attempts the government made to seek cooperation from Silicon Valley.[3]

This thesis explores the historical, political, and legislative developments that contributed to the rise of encryption in recent years, as well as constitutional doctrines

---

[1] 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/.

[2] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the Senate Judiciary Committee* (July 2015) (written statement of Sally Quillian Yates, Deputy General Counsel, FBI).

[3] Nicole Perlroth and David E. Sanger, "Obama Won't Seek Access to Encrypted User Data," *New York Times*, October 10, 2015, http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html.

that may be relevant to the public debate over possible policy solutions. Two possible solutions were examined using the policy option analysis method: (1) Amending the Communication Assistance to Law Enforcement Act (CALEA) to include encrypted communication devices and communication companies not previously covered by CALEA; and (2) passing legislation that authorizes law enforcement and intelligence agencies to perform hacking under very clear and specific circumstances with minimizing procedures and lawful warrants. Each proposed solution is examined through a lens of whether it would (1) be effective in solving the going-dark problem, (2) meet legal and constitutional standards, and (3) have the potential for political acceptability by protecting American values and striking the right balance between privacy and security.

Ultimately, this thesis recommends that policymakers enact legislation that sets out a clear legal framework under which the government is authorized to hack into devices and networks using existing vulnerabilities. Under the proposed framework, hacking is only authorized in cases where all the Fourth Amendment requirements are met, in addition to specific exhaustion and minimizing requirements. It also recommends that the U.S. government initiate a public education campaign to gain public support for some form of regulation concerning encryption in the future. The fundamental issue here is not only about the tension between privacy and security. The issue is also about who should make decisions with broad implications for the collective security: elected officials or the technology industry.

References

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

Perlroth, Nicole, and David E. Sanger. “Obama Won’t Seek Access to Encrypted User Data.” *New York Times*, October 10, 2015. http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html.

ACKNOWLEDGMENTS

I am grateful for TSA Chief Counsel Francine J. Kerner, Principal Deputy Chief Counsel Margot Bester, and Assistant Chief Counsel Steven Colon for nominating me to this CHDS master's program. I would not have been able to complete the program and this thesis with my sanity intact if it were not for the support of my immediate supervisor Jeffrey Velasco and my colleagues who picked up the slack for me with generosity and good humor.

My two thesis advisors, Carolyn Halladay and Ted Lewis, deserve tremendous credit and my utmost appreciation. Dr. Lewis spent hours listening and sometimes arguing with me so that I could see my way clearer toward a defensible position. Dr. Halladay read and reread my drafts and provided me with invaluable input. Special thanks go to Professor Chris Bellavita, who was instrumental in me selecting "going dark" as a thesis topic. Along with the excellent faculty and staff at CHDS, my friends and colleagues of Cohort 1505/1506 made the last 18 months inspiring and enjoyable. It has been a privilege to know them, and they have my affection and respect.

I owe a debt of gratitude and more to Jim Adams, whose patience, love, and support helped sustain me through many sleepless nights to meet the demands of work and this program.

Last in order but first in scale, I thank my parents for all the sacrifices they made for me over my lifetime. The genesis of all of my accomplishments is their decision to risk our lives and liberty as boat refugees to come to this country many years ago. For decades, my father worked 10- to 12- hours shifts on the assembly line, and my mother took home piecework, earning a few pennies each to put me through college and law school. In today's political climate, it is more important than ever for me to stand up and be counted among the refugees and immigrants of this country who fervently believed in its promises and ideals. More often than not, and in more ways than one, we expended blood, sweat, and tears to make contributions to our adopted homeland according to our abilities and talents. This thesis is for immigrant parents and their children.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Since the spring of 2013, when Edward Snowden leaked classified information regarding the National Security Agency's (NSA) covert collection of telephony metadata from major communication providers, Internet giants such as Apple and Google have rolled out end-to-end encryption on their devices. End-to-end encryption means that "only the recipient of the message can decrypt it and not anyone in between."[1] Today, hundreds of millions of users around the world are now enjoying end-to-end encryption on Apple iPhones, Google Chrome, Android, WhatsApp, and many other Internet platforms and applications. Indeed, a vast majority of technology providers have now designed the technology in such a way that they cannot access the data sought, even pursuant to a court order, because they do not hold the key.[2] The security situation is the same for data "at rest" on an electronic device or data "in motion" over electronic networks. This trend presents a unique challenge to the law enforcement and intelligence communities because the hallmark of their investigative tools is interception of communications that are now out of reach because of end-to-end encryption. This problem is known as "going dark."

A. PROBLEM STATEMENT

The intelligence and law enforcement communities have been locked in a debate with privacy advocates and the technology industry over this going dark problem. The central issue is whether the government should mandate "exceptional access" to solve the going dark problem created by end-to-end encryption. Mandating exceptional access means requiring the technology industry to design its encrypted software or hardware so law enforcement and intelligence agencies have access if necessary under lawful

[1] 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/.

[2] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the Senate Judiciary Committee* (July 2015) (written statement of Sally Quillian Yates, General Counsel, FBI).

warrants. This arrangement is also commonly known in the technology industry as requiring a "backdoor" to end-to-end encryption.[3]

Technologists generally oppose designing the "backdoor" or "exceptional access" to the system with the government holding the key as a solution. They claim building exceptional access into encrypted systems cannot be done without creating vulnerabilities that could eventually create significant structural damage to the Internet system.[4] Worse yet, for all the risks to the entire Internet system, "backdoor" will not stop the criminals and the terrorists from using encrypted communications platforms that are freely available over the Internet. Encrypted software is also freely available from vendors operating globally, and thus are outside of U.S. law enforcement agencies' jurisdiction.[5]

This debate is also playing out in the federal court via *FBI v. Apple*. Not long after the San Bernardino terrorist attack in December 2015, the Federal Bureau of Investigation (FBI) initiated a legal battle with Apple to unlock the iPhone 5c used by one of the terrorists who, along with his wife, killed 14 and injured 21 people. A federal magistrate in the Central District of California issued an order for Apple to assist the FBI in unlocking that iPhone. Without any specific legislation applicable to compel Apple's assistance, the FBI relied on the All Writs Act of 1789 as legal authority supporting its position. Apple opposed the order, claiming that the government's demand of a backdoor will undermine the security and privacy of all its customers. Apple also asserted that the court lacks authority to issue such an order based on the 200-plus-year-old act.[6]

---

[3] Nate Cardozo and Andrew Crocker, "Deep Dive into Crypto 'Exceptional Access' Mandates: Effective or Constitutional—Pick One," *Electronic Frontier Foundation*, August 13, 2015, https://www.eff.org/deeplinks/2015/08/deep-dive-crypto-exceptional-access-mandates-effective-or-constitutional-pick-one.

[4] Harold Abelson, et al., "Keys Under Doormats," *Communications of the ACM* 5 no. 10 (2015): 24–26.

[5] Bruce Schneier, "Back Doors Won't Solve Comey's Going Dark Problem," Lawfare, 2015, https://www.schneier.com/blog/archives/2015/07/back_doors_wont.html.

[6] *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*, "Apple Inc.'s Motion to Vacate Order Compelling Apple Inc.'s to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance," accessed February 23, 2017, https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf.

While the act's applicability does not expire because of its age, the Supreme Court (Court) has put limits on its applicability in recent years. One of the limits is the requirement that there is no other statute or regulation that can be applied in these extraordinary situations. Thus, the act cannot be used to circumvent other statutes or regulations. Clearly, the fact that the FBI had to invoke the All Writs Act in this case against Apple, and in a number of less-publicized cases in recent years, is strong evidence of a policy gap.

A week before the case was to be heard, the FBI withdrew its application because it paid a private source for a workaround solution that bypassed the locked iPhone without Apple's assistance. However, this solution can only be applied to a locked iPhone 5c running iOS 8 and not every iPhone. It did not resolve the going dark problem or bridge the policy gap.

B. RESEARCH QUESTIONS

Given the policy gap addressing the going dark problem, is there a legislative mandate that addresses both public safety and individual privacy concerns? If so, what does that mandate look like?

C. LITERATURE REVIEW

A debate implies there are two sides with opposing views on a central issue. Here, the central issue is whether the government should mandate exceptional access to solve the going dark problem created by the proliferation of end-to-end encryption. On one side is the government, represented by members of the law enforcement communities like FBI Director James Comey and New York County District Attorney Cyrus Vance. The other side is comprised of the computer scientists, academics, and technology giants represented by people like Harold Abelson, Steven Bellovin, Susan Landau, Herbert Lin, Bruce Schneier, and corporate technology giants like Apple, Google, and Facebook. The essence of each side's arguments follows.

1. Law Enforcement's Perspective

Testifying before the Senate Judiciary Committee regarding the going dark problem in July 2015, FBI Director Comey and Department of Justice (DOJ) Deputy Attorney General Yates sounded the alarm, although not for the first time, that the government had lost some ability to execute court orders for communications over the Internet because they were not covered by Communication Assistance to Law Enforcement Act (CALEA).[7] They told the committee that while the government can identify individuals who were actively being recruited to join the ranks of foreign fighters in support of Islamic State of Iraq in the Levant (ISIL) on publicly accessed social networking sites, law enforcement agents are no longer able to access the contents of these communications when these individuals are being directed by ISIL operatives to move their communications to end-to-end encrypted platforms.[8]

To highlight the challenges presented to law enforcement, Director Comey said that today's technology landscape allows suspects myriad ways to communicate and multiple options of service providers. Suspects can also switch from using mobile to Wi-Fi or voice to text. This constant switching of platforms and services gives criminals and terrorists a potential edge because it is easier for law enforcement to lose coverage of their communication.[9]

Speaking for local law enforcement at the same hearing, District Attorney (DA) Cyrus Vance for the County of New York testified that

> between October 2014 and June 2015, 35 percent of the data extracted from all phones by [his] office was collected from Apple devices; 36 percent was collected from Android devices. When smartphone encryption

[7] The Communication Assistance for Law Enforcement Act (CALEA) of 1994 required that communication service providers design software or hardware in such a way that they will be able to provide technical support to the government to conduct wiretaps under lawful warrant.

[8] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the Senate Judiciary Committee* (July 2015) (written joint statement of James Comey, FBI Director and Sally Quillian Yates, Deputy Attorney General), 4

[9] James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" (Washington, DC: Brookings Institution, October 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

> is fully deployed by Apple and Google, 71 percent of all mobile devices examined may be outside the reach of a search warrant.[10]

This fact is extremely problematic, according to Vance, because

> people live their lives today on their smartphones, which they use for, among others things, emailing, texting, taking pictures, posting pictures, shopping, conducting business, and searching the web. To investigate these 100,000 [the number of criminal cases his offices handled each year] cases without smartphone data is to fight crime with one hand tied behind our backs.[11]

In November 2015, the Manhattan District Attorney's Office released a report detailing that

> between September 17, 2014, and October 1, 2015, the Manhattan DA Office was unable to execute approximately 111 search warrants for smart phones because those devices were running iOS 8. The cases to which those devices related include homicide, attempted murder, sexual abuse of a child, sex trafficking, assault, and robbery.[12]

Furthermore, DA Vance suggested that Congress, not Apple or Google, should be the party to find the correct balance between privacy and public safety.[13]

2. Academics and Cryptographers' Perspectives

Just one day before Director Comey was to testify before the Senate Judiciary Committee in July 2015, a group of 14 world-renowned cryptographers and computer scientists published a seminal report titled *Keys Under Doormats*, detailing why mandating a backdoor for law enforcement is a bad idea.[14] The report explained their opposition to exceptional access and highlighted three major problems.

---

[10] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the Senate Judiciary Committee* (July 2015) (written statement of Cyrus Vance, Manhattan, District Attorney).

[11] Ibid.

[12] "Smartphone Encryption and Public Safety," Manhattan District Attorney's Office, November 2015, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety, 9.

[13] Ibid.

[14] Abelson et al., "Keys Under Doormats."

The first problem, the group argued, is that the security of the Internet would absolutely be undermined if exceptional access is built into the system. Security techniques such as forward secrecy can no longer be applied. "Forward secrecy" is a cryptographic protocol where decryption keys are deleted immediately. Even if the decryption key is stolen, the thief is still not able to access earlier or future communications.[15] The damage is minimized to just that particular communication. However, exceptional access requires that all data and communications be accessible and is thus incompatible with forward secrecy.

The second problem with mandating exceptional access, according to the authors of *Keys Under Doormats,* is forcing the Internet to increase system complexity. The more complex a system is, the less secure it is. Every time a new security technology is developed, hundreds of thousands of programmers would have to test it, presenting a cumbersome and time-consuming process.[16] Furthermore, new security features can interact with others to create vulnerabilities and undermine the security of the Internet in ways that can be unforeseeable.[17]

Lastly, systems with exceptional access become targets with certain and substantial rewards if successfully hacked and therefore will attract bad actors. If the government has the keys to every encrypted platform, an attacker who gained access to these keys would gain access to all, risking everyone's data on a massive scale.[18]

The authors of *Keys Under Doormats* also point out the challenges of engaging in a debate in which there is no clear and concise proposal from the government. They call on government officials to "document their requirements and then develop genuine, detailed specifications for what they expect exceptional access mechanism to do."[19] Herbert Lin, a Senior Research Scholar at the Center for International Security and Cooperation at Stanford University, agreed that the government should take the lead in

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] Ibid., 25

present design proposals. Testifying before the Senate Judiciary Committee on July 8, 2015, Dr. Lin proposed that the government present specific design proposal of a system that provides exceptional access.[20] According to Dr. Lin, only then can the government and industry have a technical debate whether a plan is workable or not, and the government can improve on its initial design based on the technical criticism.[21] As it is the government that wants exceptional access, it should be the one to bear the initial design and cost of implementation rather than passing that cost on to the providers, Lin asserted.[22]

Speaking for President Obama's Review Group on Intelligence and Communications Technology, Peter Swire left no doubt after his testimony before the Senate Judiciary Committee on July 8, 2015, that the Review Group "unanimously and clearly recommended that the U.S. government vigorously encourage the use of strong encryption."[23] Furthermore, Professor Swire seemed dismissive of the going dark problem, stating that it is more accurate to say that we are in the "golden age of surveillance rather than going dark."[24] The increase of electronic communications provides law enforcement and intelligence agencies with growing amounts of data and metadata to use. In fact, the government's biggest technical problem is analyzing the data it collected.[25] For example, the NSA estimates that it can only analyze a tiny fraction of the equivalent of 580 million file cabinets of documents it collects every day.[26] Professor Swire opined that Director Comey's statement of how widespread the going dark problem is essentially ignored the availability of data backed up on the cloud and as such,

---

[20] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the Senate Judiciary Committee* (July 2015) (testimony of Herbert Lin, Senior Research Scholar, Center For International Security and Cooperation).

[21] Ibid.

[22] Ibid.

[23] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the Senate Judiciary Committee* (July 8, 2015) (testimony of Peter Swire, Huang Professor of Law and Ethics), 2.

[24] Ibid.

[25] Daniel Byman and Benjamin Wittes. "Reforming the NSA." *Foreign Affairs*, May-June, 2014.

[26] Ibid.

simply overstated the severity of the going dark problem.[27] Professor Swire concluded that the government's inability to access contents in a fraction of these communications is an insufficient reason to compromise individual privacy as well as U.S. economic, diplomatic, and security interests.[28]

In February 2016, some of the same authors of the *Keys Under Doormats* reconvened along with a diverse group of security and policy experts in academia and the U.S. intelligence community and published a paper titled *Don't Panic*. The group did not agree on the scope of the going dark problem or on a policy recommendation that strikes the correct balance between competing interests. However, they did agree on a few findings.[29] The group found that because communication service vendors themselves need access to users' data as a part of their business models and/or to monitor and improve functionality, they are unlikely to adopt end-to-end encryption in their devices or platforms.[30] The authors also found that metadata stored on the cloud, network sensors, and the Internet of Things (IoT) technologies[31] may serve to mitigate the going dark problem.[32]

3. Technology Industry's Perspective

While cryptographers and computer scientists advocate for the security of the Internet, the technology industry is purported to be the fierce defender of individual privacy in this debate. Apple, as the most valuable company in the world at $234 billion in sales, is the public face of its industry's stance on consumer privacy after defying an order by a U.S. magistrate judge to provide reasonable assistance to the FBI to unlock a

---

[27] Testimony of Peter Swire, 7.

[28] Ibid., 3

[29] "Don't Panic Making Progress on Going Dark Debate," Berkman Center for Internet and Society and Harvard University, February 1, 2016, p.3, https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[30] Ibid., 10–11.

[31] The Internet of Things (IoT) technology refers to when appliances like refrigerators and toasters or products like watches and activities trackers are equipped with sensors or recording devices that collect and store an enormous amount of data of their surrounding environments. They also connect wirelessly to the Internet and each other and can be targets for hacking.

[32] Ibid., 11.

dead terrorist's iPhone. In an open letter to Apple's customers at the start of the *Apple v. FBI* litigation in the spring of 2016, Apple's CEO Tim Cook wrote that people use their smartphones to store very personal and private information such as financial and health data. Thus, it is natural that they would expect Apple and other technology companies to protect this data.[33] That is why Apple has been using encryption and will continue to fight against a government-mandated backdoor, he continued. Citing arguments from cryptologists and national security experts, Mr. Cook claimed that weakening encryption would only put law-abiding citizens at risk because criminals and bad actors will continue to use strong encryption.[34] Other giants of the technology industry such as Google, Amazon, Yahoo!, and Facebook not only spoke out in support of Apple's stand for consumer privacy, but also filed briefs in *Apple v. FBI* in support of Apple over other legal issues presented in the case.[35]

D. RESEARCH DESIGN AND METHODOLOGY

As reported earlier, the going dark debate presents yet another challenge for the government to strike the balance between liberty and security. The rhetoric on both sides has not served to find possible solutions despite the many attempts the government made to seek cooperation from Silicon Valley.[36] The object of this thesis is to perform a policy option analysis of two possible solutions to the going dark problem: (1) amending the Communication Assistance to Law Enforcement Act (CALEA) to include encrypted communication devices and communication companies not previously covered by CALEA, and (2) passing legislation that authorizes law enforcement and intelligence

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

[34] Ibid.

[35] Nick Wingfield and Katie Benner, "Apple Is Rolling Up Backers in iPhone Privacy Fight Against F.B.I," *New York Times*, accessed March 6, 2016, http://www.nytimes.com/2016/03/04/technology/apple-support-court-briefs-fbi.html.

[36] Nicole Perlroth and David E. Sanger, "Obama Won't Seek Access to Encrypted User Data," *New York Times*, October 10, 2015, http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html.

agencies to perform hacking under very clear and specific circumstances with minimizing procedures[37] and lawful warrants.

These two possible solutions are examined through a lens of whether each solution would (1) be effective in solving the going dark problem; (2) meet legal and constitutional standards; (3) have the potential for political acceptability by protecting American values and striking the right balance between privacy and security. Ultimately, I recommend that policymakers enact legislation to authorize hacking under limited and specific circumstances with clear judicial oversights and minimizing procedures.

This thesis focuses mainly on the going dark problem faced by law enforcement and domestic counter-terrorism agencies as the result of end-to-end encryption. Chapter I examines issues raised by both sides of this debate with the government, specifically the intelligence and law enforcement communities on one side, and technologists, cryptographers, and industry on the other. Chapter II gives a brief primer on key technological concepts as well as historical, political and social context from which encryption and the going dark problem arises. Chapter III reviews the constitutional framework that is foundational to any discussion of policy solution to the going dark problem. Chapters IV and V evaluate each of the two policy options addressing the going dark problem through three critical lenses: effectiveness in addressing the going dark problem, meeting legal and constitutional standards, and the likelihood of political acceptability. This thesis concludes with Chapter VI in which I argue and recommend legislation setting out a clear legal framework for which the government is authorized to hack into devices and networks using existing vulnerabilities. Under the proposed framework, hacking is only authorized in cases where all the Fourth Amendment requirements are met, in addition to specific exhaustion and minimizing requirements.

[37] The Federal Wiretap Act authorizes government wiretaps but also imposes a number of restrictions on the government, known as minimizing procedures, such as time limit of no more than 30 days to conduct the wiretap; the wiretap must be conducted in a way that only the material authorized is obtained; terminating the intercept as soon as material authorized is obtained, etc. See 18 U.S.C. 2518(5).

II. BACKGROUND

> Encryption technologies are the most important technological breakthrough of the last one thousand years …. Cryptology will change everything.
>
> Lawrence Lessig,
> *Code and Other Laws of Cyberspace*

Although this thesis posits that the going dark problem is a policy gap and not a technical problem, it is still helpful to have some fundamental technical background as well as the historical, political, and social context in exploring possible policy solutions to this problem.

A. DEFINITIONS

Encryption is a way of taking readable data, "plain text," and transforming it into incomprehensible strings of random bits, "crypto-text," to make the conveyed message unintelligible. To turn crypto-text into plain text or usable text, the recipient of the data has a "key," which is a string of bits mathematically arranged.[38] Data Encryption Standard (DES) was the first commercially available symmetric key standard with a 56-bit key. A 56-bit key offers more than 70 quadrillion possible combinations.[39] However, DES is no longer considered secure because it is susceptible to brute force attacks within a short time by high-computing power computers. Today, Advanced Encryption Standard (AES) has replaced DES. AES uses 128- , 192- , or 256-bit keys, and should be secure for a long time. A 128-bit key can have more than 300,000,000,000,000,000,000,000,000,000,000,000 key combinations.[40]

---

[38] President's Council of Advisors on Science and Technology. *Big Data and Privacy: A Technological Perspective.* (Washington, DC: White House, 2014).

[39] Jeff Tyson, "How Encryption Works," AllData N.S., August 15, 2016, http://alldatans.com/how-encryption-works/.

[40] Jeff Tyson, "How Encryption Works," HowStuffWorks, April 6, 2001, http://computer.howstuffworks.com/encryption.htm.

End-to-end encryption means that both parties to the communication use encryption and only those parties hold the key.[41] However, even end-to-end encryption with an Advanced Encryption Standard (AES) key is still vulnerable to man in the middle attacks. This type of attack means that a hacker can provide the AES key to one or both endpoints of the communication and intercept the encrypted communications.[42] Thus, it is necessary to add on another layer of security to any infrastructure called "authentication."

"Authentication" is a process by which one can be sure that the information sent is "authentic" and has not been tampered with by a hacker (man in the middle). To authenticate his/her identity or the information he/she is sending, a person may use a password, a pass card, or a digital signature.[43] When a user enters his/her user name and password, it is checked against a secure file for confirmation before he/she is allowed access. A pass card can be a simple card with a magnetic strip or an embedded chip. A digital signature is attached to the document, and if the document is altered in any way, the signature is invalid and the document will not decrypt.[44] Digital signatures require a public-key infrastructure (PKI) along with third-party certificate authorities that vouch for the sender and recipient as well as provide a key escrow (a system by which a key to decrypt is held in trust by a third party) for public and private keys.[45]

In encryption, a backdoor is another means to access the encrypted data, usually surreptitiously or without authorization. Encryption with a backdoor is encryption designed in such a way so that a third party (hypothetically, law enforcement) may have access to the data with some authorization by the service providers.[46] According to the

---

[41] Danielle Kehl "Encryption 101," *Slate*, February 24, 2015, http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html.

[42] Ibid.

[43] Tyson, "How Encryption Works."

[44] Ibid.

[45] Ibid.

[46] H. V. Jagadish, "Encryption, Cybersecurity, Privacy, Terrorism," Homeland Security News Wire," accessed March 4, 2016, http://www.homelandsecuritynewswire.com/dr20160224-passwords-privacy-and-protection-can-apple-meet-fbi-s-demand-without-creating-a-backdoor.

FBI, backdoor access is surreptitious or clandestine access while front-door access is access that occurs with the knowledge and assistance of the service provider. CALEA and the Foreign Intelligence Surveillance Act (FISA) presume front-door access because it is statutorily mandated.[47] The problem with backdoor access is that it must also be made secure and able to distinguish between authenticated law enforcement authorities versus hackers.

B. A BRIEF HISTORY OF ENCRYPTION

A brief history of encryption is instructive as it may provide clues for a policy solution. Encryption is not a modern-age technology. Diplomats, intelligence officers, and soldiers have used encryption methods for centuries. According to David Kahn, who wrote the authoritative history of encryption, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, during his tenure as George Washington's secretary of state, Thomas Jefferson encrypted the letters that he sent overseas using a wheel cipher—a wooden device that he invented.[48] Despite its long history, electronic encryption methods that relied on sophisticated mathematical algorithms in the 20th century were available only to members of the government, intelligence, and military communities, not the public.[49]

All that changed when researchers Whitfield Diffie and Martin Hellman published a paper in 1976 demonstrating how ordinary citizens and businesses could use encryption to keep their communications and data securely private over a public communication network.[50] Essentially, the Diffie-Hellman system separates keys into two types—a

---

[47] Responses of the FBI to Questions for the Record Arising from February 17, 2011, Hearing Before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security Regarding "Going Dark," p. 2.

[48] David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (New York: Scribner, 1996).

[49] Danielle Kehl, Andi Wilson, and Kevin Bankston, "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," New America, 2, https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf.

[50] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, IT-22, November 6, 1976. It was later called the "Diffie-Hellman Key Exchange."

public key that is used to encrypt and a private key that is used to decrypt. It is the basis for the PKI system used on the Internet. It also depends on a secure and reliable certificate authority to issue keys via certificates. Theoretically, the Institute of Electrical and Electronics Engineers (IEEE) X509 standard guarantees authentication, integrity, confidentiality, and non-repudiation. The IEEE X509 standard allowed online encryption to grow exponentially as demands for secure communications among ordinary citizens increase.[51] Since encryption became available to the public through the Diffie-Hellman method, intelligence and military officials have been viewing the widespread use of encryption as a threat to national security.[52] This concern led to the Crypto Wars of the 1990s.

1. The Crypto Wars of the 1990s

The debate surrounding the going dark problem as it related to encryption and mandated government's access is not new. Some of the arguments are recycled and the vehemence with which they are presented is revived from the first Crypto Wars of the 1990s. The Crypto Wars refer to a period in the 1990s when there was a standoff between technologists and the government over two major battles: the proposed mandatory use of the Clipper Chip and U.S. policies regarding export controls on encryption technology.[53]

a. Clipper Chip

The Clipper Chip was a government-designed technology and introduced by the Clinton Administration in 1993 as an effort to compromise between the public's need for strong encryption and law enforcement's need to access unencrypted communications.[54] This system provided a "key" to the government to decrypt the communications under lawful court orders. As a check and balances measure, the "key" would be split in two so that no single government entity can abuse its authority and misuse the key to conduct an unauthorized wiretap. This idea of splitting the key came to be known as the "key

[51] Kehl, et al., "Doomed to Repeat History," 3.

[52] Ibid.

[53] Ibid., 5–15.

[54] Ibid.

escrow" system.[55] The Clipper Chip worked as follows: It contained a Law Enforcement Access Field (LEAF) that holds the encryption device serial number and a decryption key. If and when law enforcement officials obtained a valid wiretap order, they can use the key and the information in the LEAF to decrypt the encrypted messages.[56]

As Danielle Kehl, Andi Wilson, and Kevin Bankston recounted in *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s,* the proposal faced opposition from privacy advocates, cryptographers, and technology industry leaders who were concerned about creating vulnerability in the system by providing the government (a third party to the communications) a key and thereby unprecedented access to private information of the citizenry. They were also concerned about the economic impact given the mandatory nature of the Clipper Chip. If the Clipper Chip was to be mandatorily built in every device and platforms, this proposal was the government's first step toward prohibiting other forms of encryption.[57]

The debate continued until 1994 when Matthew Blaze, a researcher at Bell Labs, uncovered a major technical flaw in the Clipper Chip rendering the proposal effectively dead.[58] Blaze found that the LEAF could be manipulated to give the wrong key so that the encrypted message cannot be properly decoded.[59]

However, the idea of software key escrow, where private companies would implement a key to software products held by a third party, persisted well into the 2000s and even today.[60] Current X509 certificates and the certificate authorities that support PKI are essentially online key escrow databases under control of the private sector instead of the government.

---

[55] Ibid., 5.

[56] Sharon Begley, "Foiling the Clipper Chip," *Newsweek*, June 12, 1994, http://www.newsweek.com/foiling-clipper-chip-188912.

[57] Kehl et al., "Doomed to Repeat History," 6.

[58] Ibid., 5

[59] Begley, "Foiling the Clipper Chip."

[60] Abelson, et al., "Keys Under Doormats," 7.

b. Communication Assistance for Law Enforcement Act

Perhaps because the government was losing the Clipper Chip battle, Congress enacted the CALEA in 1994 to address concerns from law enforcement that they were losing their capabilities to access communications due to the United States moving from analog to digital communications. Testifying before the House of Representatives Judiciary Committee in 2011, the FBI General Counsel, Valerie Caproni, explained that the impetus of CALEA was to ensure that the government be able to intercept electronic communications with a search warrant.[61] The law required that communication service providers design software or hardware in such a way so they are able to provide the government technical support when called upon to do so.[62]

Originally, CALEA only applied to traditional telephony and mobile telephone services, but through the Federal Communication Commission's (FCC) authority under rule making, it was expanded to include facilities based on broadband Internet access—Internet Service Providers (ISP) and Voice over Internet Protocol (VoIP) services such as Skype.[63] Nevertheless, CALEA still did not cover webmail, social networking sites, or peer-to-peer services such as chat or instant messaging platforms like WhatsApp.[64]

c. Export Controls of Encryption Technology

Another significant battle during the Crypto Wars of the 1990s was the battle over export controls on encryption technology. Prior to 1996, cryptographic tools were classified as munitions and were listed on the U.S. Munitions List (USML), and their disseminations and use were controlled under the International Traffic in Arms Regulations (ITAR). This classification was because they were used almost exclusively by intelligence agencies and the military, historically.[65] These controls were put in place

---

[61] *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing before the U.S. House of Representative, Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security (*February 17, 2011) (testimony of Valerie Caproni, General Counsel of the FBI) 13.

[62] Ibid.

[63] "Electronic Frontier Foundation," CALEA, https://eff.org/issues/calea

[64] Testimony of Valerie Caproni, 13.

[65] Danielle Kehl et al., "Doomed to Repeat History," 12.

in the hope of delaying the widespread adoption of strong encryption technology abroad that may lead to the government's diminished capability to gather foreign intelligence.

By the end of the 20th century, it became clear that encryption export controls did not effectively serve the intended purposes. Yet they had the unintended and unwanted consequence of hurting U.S. businesses and undermining the country's economic interest.[66] Thus, it became harder and harder for the government to justify this policy. Finally, on September 16, 1999, the White House announced that it would update encryption export controls policy to remove virtually all restrictions.[67]

CALEA notwithstanding, by 2000, cryptologists, commercial technology companies, and privacy rights advocates declared victory in the Crypto Wars. Ultimately, the lessons from the first Crypto Wars were one of the causes of the government's defensive postures in approaching the going dark problem.

2. 9/11 Terrorist Attacks

For purposes of this thesis, there are two major U.S. responses to the 9/11 terrorist attacks that had the most direct effect on the current going dark debate. They are certain key amendments of the Foreign Intelligence Surveillance Act, specifically Sections 206 and 215 of the U.S.A. Patriot Act, and the FISA Amendment Act of 2008.

a. The Birth of the Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act of 1978 is a statutory framework established to govern foreign intelligence gathering using wiretaps, physical searches, pen registers, trap and trace devices, and accessing business records or other tangible things.[68] FISA of 1978 was enacted after the Supreme Court ruled that a warrant was required for a wiretap in domestic national security threats cases but leaving open the question of the Executive Branch's power to order wiretappings against foreign security

---

[66] Ibid., 14.

[67] Ibid., 16.

[68] Edward C. Liu "Reauthorization of the FISA Amendment Act" (CRS Report No. 42725) (Washington, DC: Congressional Research Service, 2013) 1.

threats.[69] FISA of 1978 specifically established that electronic surveillance in the United States without satisfying the Fourth Amendment probable cause requirement is only to be used to collect non-criminal foreign intelligence and counterintelligence against a foreign person or foreign agent. In addition, it created a foreign intelligence surveillance court (FISC) that would grant warrant orders upon the government's application and the U.S. Foreign Intelligence Surveillance Court of Review. Perhaps most urgently, it articulated a probable cause standard under which surveillance warrants may be granted to collect foreign intelligence.[70] Because the Court ruled in *United States. v. Verdugo-Urquidez* that the Fourth Amendment protection does not apply to a non-U.S. person who does not have strong ties to the United States, FISA is the *de facto* Fourth Amendment limitation on government's domestic collection of electronic data from foreign nations or agents of foreign nations.[71]

b. The Evolution of FISA

In 1995, Congress amended FISA to include physical searches. Congress again amended FISA in 1998 to authorize installation of a pen register and trap-and-trace devices. This new authority was also extended to cover emails and electronic communications.[72] Originally, FISA was interpreted that surveillance evidence obtained under a FISC warrant was not to be shared for criminal prosecution. This interpretation was due to the original FISA requirement that the government certify that the purpose of a wiretap is for foreign intelligence only.

In immediate response to 9/11, Congress passed the USA Patriot Act in October 2001, Section 206 of which amended FISA to explicitly enable intelligence sharing and cooperation between foreign intelligence and law enforcement. Section 206, also commonly known as a "roving wiretap" provision, permits a FISC to issue a general

---

[69] *United States v. United States Dist. Court for Eastern Dist. of Mich*., 407 U.S. 297 (Supreme Court 1972).

[70] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §1801 et. seq.

[71] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 275A (1990).

[72] James G. McAdams III, "Foreign Intelligence Surveillance Act (FISA): An Overview," https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf.

order of assistance to any communication providers, so that if a suspect changes providers, law enforcement does not have to seek a new order.[73] Furthermore, Section 206 of the USA Patriot Act lowered the threshold for a FISA warrant. Instead of collecting foreign intelligence being *the* [sole] purpose, this section now only required foreign intelligence to be a "significant purpose" of the warrant. Law enforcement and national security agencies may also now share intelligence under this provision.[74] In this sense, the authority to conduct electronic surveillance under FISA is not extended to law enforcement for the common purpose of *investigating* criminal enterprises and activities. However, evidence obtained under a FISC warrant may be shared with law enforcement in *prosecuting* crimes.[75]

Section 215 of the USA Patriot Act also enlarged the government's authority to seek an order from the FISC for production of any tangible things, including but not limited to business records, documents, and in today's technology-driven communications to include emails, texts, tweets, photographs, contacts backed up in the clouds or stored within an electronic device.[76]

In late 2005, the *New York Times* reported that after 9/11, President George W. Bush secretly authorized the NSA to conduct warrantless interceptions of emails and phone calls of Americans and others in the United States in an effort to monitor "dirty numbers" linked to Al Qaeda.[77] The program was controversial because it represented a departure from the NSA's past practices and constitutional safeguards. In the past, the NSA was able to intercept phone calls and emails that originated on foreign soil, but must obtain a warrant for same if originated in the United States. Under this program, the NSA began to monitor calls and emails from individuals inside to the United States to

---

[73] Liu "Reauthorization of the FISA Amendment Act," 7.

[74] Glen Sulmasy and John Yoo, "Katz and the War on Terrorism," *UC Davis Law Review* 41, no. 3 (2008): 1227. http://lawreview.law.ucdavis.edu/issues/41/3/intl-crime-terrorism/41-3_Sulmasy-Yoo.pdf.

[75] Ibid.

[76] 50 U.S.C. §1861(a)(1) as cited in McAdams, "History of Foreign Intelligence Surveillance Act (FISA)," 9.

[77] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

recipients overseas through a series of connections with a suspected terrorist phone numbers.[78] While *United States. v. Verdugo-Urquidez* permitted warrantless wiretaps on non-U.S. persons, the Fourth Amendment does not permit warrantless wiretaps on U.S. citizens, permanent residents, and those residing in the United States.

In an effort to legalize President Bush's controversial program, Congress amended FISA again in 2008 by adding Title VII to FISA.[79] The new Title VII of FISA authorized surveillance on non-U.S. persons without court orders. On the other hand, Congress also explicitly required court orders for surveillance of U.S. persons abroad and established procedures for both.[80]

Also significant in the FISA Amendment Act of 2008 is the encrypted data retention provision. Under Section 702, the NSA may retain encrypted communications indefinitely. While unencrypted communications may be retained for only five years from the date the collection is authorized, encrypted domestic communications may be retained "for any period of time" during which the encrypted communications is being used for cryptanalysis.[81] For foreign communications of a U.S. person, the NSA retains encrypted communications for a "period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement."[82]

c. FISA as Applied

Under FISA, the government may be granted a warrant for surveillance by the FISC upon certifying that the *suspect* is connected to a foreign power, including a

---

[78] Ibid.

[79] Beth Rowan, "Post 9/11 Changes by the U.S. Government," InfoPlease, accessed September 30, 2015, http://www.infoplease.com/us/history/911-anniversary-government-changes.html.

[80] Liu, "Reauthorization of the FISA Amendment Act" p. 2.

[81] Cryptanalytic is the process of deciphering encrypted messages without the key.

[82] Nat'l Sec. Agency/Cent. Sec. Serv., Exhibit B: Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended § 3(b)(4) (2011), available at In the Matter of the Search of an iPhone, as cited in Laura K. Donahue, "Section 702 and the Collection of International Telephone and Internet Content," *Harvard Law Journal and Public Policy* 38 (2015): 117, 199.

terrorist organization. The government must also certify that the surveillance is for a national security intelligence *purpose*.[83] The government's application is *ex parte*, which means the opposition does not need to be present and FISC proceedings are closed to the public. Much has been made about the secrecy of the FISC,[84] when in truth it serves an important national interest by allowing the government to present classified information—so that the target or defendant can challenge this evidence—without having to publicly disclose classified information.[85] Furthermore, necessary safeguards have also been put in place if and when evidence obtained through a FISC warrant is being used in a criminal proceeding. Consider the following:

First, the attorney general and no one else may approve the use of FISA evidence in a criminal proceeding.[86] Second, the government must also notify the defendant and the court of its intention to use FISA evidence.[87] At this juncture, it is highly likely that the defendant will raise an objection and move to suppress the evidence. Third, if the defendant moves to suppress, the government's application to the FISC and the resulting FISA evidence must be disclosed to the presiding judge for *in camera* review.[88] If the judge is satisfied that the FISA evidence within the scope of the government's application and the evidence is lawfully obtained under the FISC's order, the FISA evidence will be admissible. Lastly, if the defendant's motion to suppress is granted, the statute provides for the government to either withdraw its FISA evidence or provide its FISC application to the defendant.[89]

---

[83] 50 U.S.C. § 1804

[84] Glen Greenwald, "FISA Court Oversight: A Look Inside a Secret and Empty Process," *Guardian*, June 18, 2013, https://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy (the NSA is required to submit a report to the FISC annually of its general procedures of how to decide whom they can eavesdrop without a warrant, but because the FISC court operates entirely in secret, the NSA's reports are never revealed and independently verified); Dia Kayyali, "What You Need to Know About the FISA Court and How It Needs to Change," Electronic Frontier Foundation, August 15, 2014, https://www.eff.org/deeplinks/2014/08/what-you-need-know-about-fisa-court-and-how-it-needs-change. (The Court operates in secret and has to rely on one-sided information provided by the government.)

[85] Sulmasy and Yoo, "Katz and the War on Terror," 1226.

[86] McAdams III, "History of Foreign Intelligence Surveillance Act (FISA).," 9.

[87] Ibid.

[88] Ibid.

[89] Ibid.

d. FISA in Numbers

The Department of Justice reported in its annual report to Congress that in the calendar year 2015, out of the 1,499 applications the government made to the FISC for electronic surveillance and physical searches, 1,457 of them were for electronic surveillance. None of these applications were denied and only 80 orders were modified.[90] There were 142 applications for access to business records and production of tangible things in the same calendar year. Again, none was denied and only five orders were modified.[91] What remains unclear about these numbers is whether the government was able to obtain the data that they sought and how many of their requests were thwarted by end-to-end encryption and the going dark problem.

On December 30, 2012, President Obama signed H.R. 5949, the FISA Amendments Act Reauthorization Act of 2012, which extends Title VII of FISA until December 31, 2017.[92] Therefore, any proposed solution to the going dark problem must take into account the requirements of Title VII of FISA to conduct surveillance of U.S. persons abroad, especially in cases of remote hacking and wiretaps.

3. The Rise of Encryption Post-Snowden's Revelations

There is no question that the Snowden revelations in June 2013 had profound effects on the work of intelligence and law enforcement agencies. In May 2014, the technology company Recorded Future[93] reported:

> Following the June 2013 Edward Snowden leaks we observe an increased pace of innovation, specifically new competing jihadist platforms and three major new encryption tools from three different organizations—

90 "FISA Annual Report to Congress for CY 2015," U.S. Department of Justice, April 28, 2016, http://www.fas.org/irp/agency/doj/fisa/2015rept.pdf.

91 Ibid.

92 Ibid.

93 Recorded Future is a technology start-up based out of Somerville, Massachusetts. They call themselves the "Real Time Threat Intelligence Company." Their analytic tool scours the hundreds of thousands of sites, blogs, and Twitter accounts on the web and analyzes the connection between people, entities, and events. In July 2010, *Wired* magazine reported that they obtained investments from Google and the CIA. Noah Shatchman, "Exclusive: Google, CIA Invest in 'Future' of Web Monitoring," *Wired*, July 28, 2010.

> Global Islamic Media Front, Al-Fajr Technical Committee, and ISIS—within a three- to five-month time frame of the leaks.[94]

In September 2013, the Global Islamic Media Front released a new encryption program on mobile devices.[95] The al-Fajr Technical Committee, well known as the al-Qaeda propaganda machine, also released multiple versions of programs to encrypt emails, text and instant messages.[96] The Islamic State of Iraq and ash-Sham (ISIS) released another encryption program called Asrar al-Ghurabaa in November 2013.[97] Reported Future confirmed that al-Qaeda used encryption to release propaganda and recruitment.[98] Reported Future also found that these new encryption programs used off-the-shelf algorithms, such as Twofish, developed by cryptology expert Bruce Schneier.[99]

Meanwhile, a mood of greater intransigence from the technology industry toward the government's warrants markedly increased because they did not want to be seen as being the government's puppets after the Snowden fallout. To allay fear of the government's invasion of privacy, Microsoft announced in January 2014 that it might lease servers located outside the United States to foreign customers to store their personal data.[100] Tech giants like Google, Microsoft, Apple, Yahoo!, and WhatsApp provided automatic default encryption for users.[101] Apple announced in September 2014 that it had designed its devices running on operating system iOS 8 with end-to-end encryption so that they cannot be cracked with government search warrants.[102] Google made the

---

94 "How Al Quaeda Uses Encryption Post Snowden, Part 1," Recorded Future, May 8, 2014, https: www.recordedfuture.org.

95 Ibid.

96 "Al-Fajr Technical Committee Releases Android App for Secure Communication, Announces New website," MEMRI Cyber & Jihad Lab, June 11, 2014, https: http://cjlab.memri.org.

97 Ibid.

98 Recorded Future, "How Al-Qaeda Uses Encryption Post-Snowden, Part 1."

99 "How Al-Qaeda Uses Encryption Post-Snowden, Part 2," Recorded Future, August 1, 2014, https:www.recordedfuture.org.

100 Robin Simcox, "Surveillance After Snowden," *Henry Jackson Society*, 2015, 62.

101 Ibid., 63.

102 Craig Timberg, "Apple Will No Longer Unlock Most iPhones, iPads for Police, Even With Search Warrants," *Washington Post*, September 14, 2014.

same announcement a few days later about its latest Android operating system.[103] The effects of Apple's design decision are staggering. As of mid-2015, more than 85 million Apple devices in the United States are likely off limits to law enforcement because of default encryption.[104] This trend also affects an estimated 463 million iOS devices in used worldwide.[105]

In October 2015, the *Washington Post* reported that "White House officials have backed away from seeking a legislative fix to deal with the rise of encryption on communication devices, and they are even weighing whether to publicly reject a law requiring firms to be able to unlock their customers' smartphones and apps under court order."[106] This development is consistent with the recommendations of the Review Group on Intelligence and Communications Technologies that President Obama appointed shortly after the Snowden leaks. The Review Group's Recommendation No. 29 reads:

> We recommend that, regarding encryption, the U.S. government should:
>
> (1) fully support and not undermine efforts to create encryption standards;
>
> (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and
>
> (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.[107]

---

[103] Craig Timberg, "Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police." *Washington Post*, September 18, 2014.

[104] Don Resinger, "iPhones In Use in the U.S. Rise to 94M, New Study Suggests," CNET, May15, 2015, 10:18 AM, http://cnet.co/1RxlMCW, as cited in Jamil Jaffer and Daniel Rosenthal, "Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge," *Catholic University Journal of Law and Technology* 24, no. 2 (May 24, 2016): 289.

[105] Tomi Ahonen, "Smartphone Wars: Q3 Scorecard—All Market Shares, Top 10 Brands, OS Platforms, Installed Base," Communities Dominate Brands, October 30, 2015, http://communities-dominate.blogs.com/brands/2015/10/smartphone-wars-q3-scorecard-all-market-shares-top-10-brands-os-platforms-installed-base.html.

[106] Ellen Nakashima and Andrea Peterson. "Obama Faces Growing Momentum to Support Widespread Encryption." *Washington Post*, September 16, 2015.

[107] Richard, Clarke, Michael Morell, Jeffrey Stone, Cass Sunstein, and Peter Swire, "Liberty and Security in a Changing World, Report and Recommendations from the President's Review Group on Intelligence and Communications Technologies," December 12, 2013. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

The *Post* also obtained a National Security Council draft Options Paper on Encryption that included three recommended options for President Obama. The recommendations are to "disavow legislation and other compulsory actions; defer on legislation and other compulsory actions; or remain undecided on legislation or other compulsory actions."[108] Soon after the *Post*'s report, President Obama officially announced that his administration would not pursue legislation mandating a backdoor for law enforcement. This decision was widely seen as a victory for technologists and privacy advocates.[109]

However, since the very public legal battle of *Apple v. FBI*, President Obama had come out publicly in support of the FBI. Speaking at the South by Southwest Interactive conference in Austin, Texas, on March 11, 2016, President Obama said that the view that your smartphone is sacrosanct does not strike the balance that we as Americans have lived for 200, 300 years. "It's fetishizing our phone above every other value."[110] He called for the technology industry and law enforcement to work together toward a technological solution that strikes the right balance between our fundamental values.[111]

Not more than a few weeks after President Obama spoke on the issue, the government withdrew its request for a court order compelling Apple to assist in unlocking the terrorist's phone. In a very short filing in *Apple v. FBI*, the government said it had successfully unlocked the phone and no longer required Apple's assistance.[112] In subsequent days and weeks, it was revealed that the FBI had paid a group of professional

---

[108] "Draft Options Paper on Strategic Approaches to Encryption," National Security Council, 2015, accessed May 13, 2016. https://assets.documentcloud.org/documents/2426450/read-the-nsc-draft-options-paper-on-strategic.pdf.

[109] Issie Lapowsky, "After Paris, Encryption Will Be a Key Issue in the 2016 Race," *Wired*, November 17, 2015.

[110] Laura Sydell, "In Apple Security Case, Obama Calls To Strike A Balance," NPR.org, accessed March 14, 2016, http://www.npr.org/2016/03/12/470194268/in-apple-security-case-obama-calls-to-strike-a-balance.

[111] Ibid.

[112] Katie Benner and Eric Lichtblau, "U.S. Says It Has Unlocked iPhone Without Apple," *New York Times*, accessed March 29, 2016, http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.

hackers, or more euphemistically referred to as "security researchers," close to a $1 million for the technique to unlock the phone.[113]

4. Failed Legislative Actions

Since the San Bernardino terrorist attack and the *Apple v. FBI* litigation, there had been two legislative attempts in the United States at addressing the going dark problem. On February 29, 2016, Senator Mark Warner (D-VA) and House Homeland Security Committee Chairman Michael McCaul (R-TX) introduced the Digital Security Commission Act of 2016. The bill sought to establish a National Commission on Security and Technology Challenges in the legislative branch to examine "the intersection of security and digital security and communications technology in a systematic, holistic way."[114] The commission was to provide several interim reports and a final report on encryption issues such as how encryption is used if current warrant procedures regarding encryption should change and what it means for the security of the Internet to provide the government with exceptional access.[115]

The bill had some support in the Senate and the House but was opposed by the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU). The EFF argued that the questions this commission is tasked to answer have already been asked and answered during the first Crypto War of the 1990s.[116] The ACLU opposed the commission's subpoena authority and overbroad power to recommend changes to the

---

[113] Ellen Nakashima, "FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone," *Washington Post*, April 12, 2016, https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

[114] Digital Security Commission Act of 2016, S. 2604, 114th Cong. (2016), https://www.congress.gov/bill/114th-congress/senate-bill/2604/text; H.R. 4651, 114th Cong. (2016), https://www.congress.gov/bill/114th congress/house-bill/4651/text.

[115] Ibid.

[116] Mark Jaycox, "EFF Opposes McCaul-Warner Encryption Commission," Electronic Frontier Foundation, March 16, 2016, https://www.eff.org/deeplinks/2016/03/eff-opposes-mccaul-warner-encryption-commission.

warrant and wiretap statutes.[117] In the end, the bill never made it out of committee and died at the end of the 114th Congressional session.

The second legislative attempt regarding encryption fared no better fate. In fact, it was never formally introduced. Senator Dianne Feinstein (D-CA) and Richard Burr (R-NC) circulated a discussion draft of the Compliance with Court Order Act of 2016 (CCOA) in April 2016 in response to Apple's refusal to assist the FBI despite a court order. The draft bill required device and software manufacturers, electronic communication, and computing services to "provide responsive, intelligible information or data, or appropriate technical assistance to a government pursuant to a court order."[118] It did not require a backdoor for law enforcement or specify how the "performance standard" of providing assistance is to be met. It did allow for reimbursement of costs and provided limits that court orders would be issued under this bill only in connection with the following crimes:

1. A crime resulting in death or serious bodily harm or a threat of death or serious bodily harm.
2. Foreign intelligence, espionage, and terrorism, including an offense listed in chapter 113B of title 18, United States Code.
3. A Federal crime against a minor, including sexual exploitation and threats to physical safety.
4. A serious violent felony (as defined in section 3559 of title 18, United States Code).
5. A serious Federal drug crime, including the offense of continuing criminal enterprise described in section 408 of the Controlled Substances Act (21 U.S.C. 848).
6. State crimes equivalent to those in subparagraphs (A), (B), (C), (D), and (E).[119]

---

[117] Neema Singh Guliani, "4 Problems With Creating a 'Commission on Encryption,'" Washington Markup, March 9, 2016, https://www.aclu.org/blog/washington-markup/4-problems-creating-commission-encryption.

[118] "Feinstein Burr Draft Encryption Bill 04–2016," 114th Congress, Second Session, accessed April 11, 2016, https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf.

[119] Ibid.

The bill failed to garner any congressional support and was very heavily criticized by technologists and advocacy groups for being "flawed and dangerous," "naïve," "ludicrous," and "technically illiterate."[120] The draft proposal has not since been modified or recirculated.

[120] Greenberg, "The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate.'"

III. CONSTITUTIONAL FRAMEWORK

> Liberty and security can be reconciled; and in our system they are reconciled within the framework of the law.
>
> —*Boumediene v. Bush*, 553 U.S. 723, 798 (Sup. Ct. 2008).

Both sides of the going dark debate have invoked the Constitution, specifically the First and Fourth Amendments, either as authority in support of their position or prohibition of the other side's position. Technologists and the technology industry have invoked the First Amendment, arguing that any attempt to regulate encryption is an attempt as regulating speech and therefore runs afoul of their right to free speech. The government has invoked the Fourth Amendment as a stringent standard it has met to gain legitimacy for their need to conduct surveillance. Privacy rights advocates have invoked the Fourth Amendment as protection against government's surveillance. Thus far, the Supreme Court seems to recognize a national security exception under the Fourth Amendment but is less inclined to do so under the First Amendment. An examination of landmark First and Fourth Amendments cases will be helpful in determining whether these arguments will pass constitutional scrutiny, particularly when policy proposals this thesis analyzes will be supported or opposed based on similar arguments.

A. THE FIRST AMENDMENT

In the context of the going dark problem, First Amendment challenges arise out of the government's efforts to either regulate encryption codes or compelling decryption codes. The question of whether encryption is considered speech has been decided by a few circuit courts with different outcomes. The Supreme Court has yet to weigh in on this issue. Furthermore, it is not at all clear what the Supreme Court's view is and what standard of review the Court will apply when considering a First Amendment challenge of the government's response to the going dark problem by regulating encryption code and software.

1. General Principles of the First Amendment

The First Amendment provides: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."[121] In short, the First Amendment guarantees the freedom of religion, of free speech, of association, and of petition for redress. This thesis focuses on the free speech clause of First Amendment and discusses how the Court viewed computer algorithms, and whether the government's attempt to regulate encryption code might implicate the free speech clause.

The first and most important principle of First Amendment jurisprudence is freedom of speech is not absolute. "The First Amendment was not intended to protect every utterance."[122] It does not protect every category of speech. Over the years, the Supreme Court has excluded a few categories of speech from First Amendment protection: speech that inflicts injury or incites immediate violence,[123] defamation,[124] obscenity,[125] child pornography,[126] and virtual child pornography.[127] Yet, there is no national security exception to the First Amendment.

Of the categories that the First Amendment protects, it does not protect all equally. Commercial speech is protected to a lesser degree than political speech. While "debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials,"[128] such commercial speech as advertising is afforded a lesser

---

[121] U.S. Constitution, Amendment I.

[122] *Roth v. United States*, 354 U.S. 476 (Supreme Court 1957).

[123] *Chaplinsky v. New Hampshire*, 315 U.S. 568 (Supreme Court 1942); *Brandenburg v. Ohio*, 395 U.S. 444 (Supreme Court 1969).

[124] *New York Times Co. v. Sullivan*, 376 U.S. 254 (Supreme Court 1964).

[125] *Roth v. United States*, 354 U.S. 476 (Supreme Court 1957); *Miller v. California*, 413 U.S. 15 (Supreme Court 1973).

[126] *New York v. Ferber*, 458 U.S. 747 (Supreme Court 1982).

[127] *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (Supreme Court 2002).

[128] *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (Supreme Court 1964).

measure of protection. Commercial speech protections "commensurate with its subordinate position in the scale of First Amendment values, while allowing modes of regulation that might be impermissible in the realm of noncommercial expression."[129] Not all speech has the same value under the Constitution, according to the Court. Political debate has more value in a democracy than commercial speech. Therefore, the Court will afford a higher level of protection to political speech than commercial speech.

Government actions that infringe on political speech are subject to strict scrutiny, which requires the government to show that the regulation "furthers a compelling state interest *and* is narrowly tailored to achieve that interest."[130] In contrast, regulations on commercial speech are reviewed under intermediate scrutiny. The Court in *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of NY* held that misleading commercial speech or speech concerning unlawful activity may be regulated by the government. In this case, the New York Public Service Commission (Commission) banned advertising that promoted the use of electricity because of a 1973 fuel shortage. When the shortage was over a few years later, the Commission still continued the ban although it recognized that the ban was not a perfect means to conserve energy. Central Hudson Gas & Electric filed suit, alleging the Commission violated the First Amendment by restraining commercial speech.[131] The Court devised a three-part test for the regulation to be declared constitutional once it had been determined that the speech fell within constitutional protection: "the government must have a substantial interest in its regulation; the government must demonstrate that the restriction directly and materially advances that interest; and the regulation must be narrowly drawn."[132] The Court found that the Commission's ban did violate the First Amendment in restraining commercial speech.

---

129 *Ohralik v. Ohio State Bar Assn.*, 436 U.S. 447 (Supreme Court 1978).

130 *Citizens United v. Federal Election Com'n,* 130 S. Ct. 876, 898 (Supreme Court 2010).

131 *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of NY,* 447 U.S. 557, 559–561 (Supreme Court 1980).

132 Ibid., 566.

Although commercial speech is not afforded the greatest protection, the Commission still had to show that it had a substantial interest in conserving electricity. The Court found that it did enunciate a substantial interest because of the country's dependence on foreign energy sources.[133] Yet the Court invalidated the ban because it was not narrowly drawn to advance the interest in conservation. The Commission's ban went too far in that it also restricted advertising for products that caused no net increase in energy consumption.[134] As *Central Hudson* demonstrated, the challenge in passing constitutional muster in commercial speech cases is not in articulating a substantial government's interest, but in demonstrating that the regulation was narrowly tailored to advance that state's interest.

First Amendment scrutiny does not always turn on the type of speech regulated but also on the type of regulation imposed. Strict scrutiny is applied to content-based regulations while only intermediate scrutiny is required to review content-neutral regulations.[135] Writing the opinion for the majority, Justice Kennedy wrote:

> The principal inquiry in determining whether a regulation is content based or content neutral is whether the government has adopted a regulation because it agrees or disagrees with the message conveyed…A regulation that favors speech on the basis of ideas or views express is content based. By contrast, a regulation that favors speech without reference to the ideas expressed is content neutral.[136]

This principle is demonstrated in *Turner Broadcasting System v. FCC*, a 1994 case in which the Court applied intermediate scrutiny to the regulation that required cable systems to carry local commercial and public broadcast stations. The Court found that the rule was consistent with the First Amendment because it conferred benefits and imposed burdens without any reference to the content of the speech.[137] But just because a regulation is content neutral on its face does not end the inquiry. The Court also

---

[133] Ibid., 568.

[134] Ibid., 570.

[135] *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 642 (Supreme Court 1994).

[136] Ibid., 643.

[137] Ibid., 644.

examined the purpose of the rule and found that its manifested purpose was not to regulate the content of speech "but to keep television programming for 40% of Americans without cable."[138]

Specific to this thesis, any analysis of whether any legislative action to resolve the going dark problem will violate the First Amendment has to start with whether encryption is speech and if so, which category of speech as that will partly inform the standard of review that will be applied? Three cases decided during the first Crypto War of the 1990s might be instructive: *Karn v. U.S. Department of State*, *Junger v. Daley*, and *Bernstein v. DOJ*.

2. Encryption Source Code as Speech

As discussed in the preceding chapter, encryption code was considered a munition and its export heavily regulated until the late 1990s. These three cases challenged the government's export controls of encryption, as well as the general prohibition against publication and dissemination of encryption source code. The source code is the text of a high-level programming language. It can be used to express an idea and can be read by a human. A source code is not useful for a machine until it is translated or compiled into a lower level machine language.[139]

In *Bernstein v. DOJ*, the court considered the precise question of whether source code is speech and if so, did the government's export controls regulations constitute impermissible prior restraint on protected speech. While he was a graduate student, Daniel Bernstein developed an encryption method he called Snuffle, which he wrote in two different forms: a high-level computer programming language (source code) and the instruction of how to write this source code in prose form. He was told he could not publish his work on Snuffle in academic journals without a license because encryption code was munitions, subject to export regulations at the time.[140] He filed suit alleging First Amendment violation, among other legal theories. The District Court of the

[138] Ibid., 646.

[139] *Bernstein v. U.S. Dept. of Justice*, 176 F. 3d 1132, 1140 (Court of Appeals, 9th Circuit 1999).

[140] Ibid., 1136.

Northern District of California found that source code was speech and the government's regulations were prior restraints on Bernstein's First Amendment right.[141] The Ninth Circuit Court of Appeal agreed, holding that source code was expressive and therefore is entitled to First Amendment protection under the prior restraint doctrine.[142]

Prior restraint is government's actions, regulations, or rules that infringe upon speech prior to publication or dissemination. The Supreme Court deems prior restraint of speech to be "the most serious and the least tolerable infringement on First Amendment rights."[143] "Any prior restraint on expression comes to this [Supreme] Court with a 'heavy presumption' against its constitutional validity."[144] Nevertheless, it is possible for the presumption to be overcome with a showing of stringent procedural safeguards. It may also be overcome with the national security exception if it seeks to restrain a "clear and present danger."[145] However, because the test for "clear and present danger" announced in *Brandenburg v. Ohio* required showing imminent violence, danger, or harm, it is doubtful that any regulations addressing the going dark problem can meet this definition.[146]

With respect to *Bernstein*, the Court applied three factors for determining the validity of the licensing scheme: the scheme must be brief in duration, judicial review must be available and expeditious, and burden of bringing the case to court and the burden of proof must be with the censor.[147] Finding that the challenged regulations "grant boundless discretion to government officials and lack the required procedural

---

[141] *Bernstein v. U.S. Dept. of State*, 922 F. Supp. 1426 (Dist. Court 1996); *Bernstein v. U.S. Dept. of State*, 945 F. Supp. 1279 (Dist. Court 1996).

[142] *Bernstein v. U.S. Dept. of Justice*, 176 F. 3d 1132, 1141 (Court of Appeals, 9th Circuit 1999).

[143] *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (Supreme Court 1976).

[144] *Organization for a Better Austin v. Keefe*, 402 U.S. 415, 419 (Supreme Court 1971); *Carroll v. Princess Anne*, 393 U.S. 175, 181 (Supreme Court 1968).

[145] *Wood v. Georgia*, 370 U.S. 375, 385 (Supreme Court 1961).

[146] *Brandenburg v. Ohio,* 395 U.S. 444 (Supreme Court 1969).

[147] *Freedman v. Maryland*, 380 U.S. 51, 58–60 (Supreme Court 1965).

protections," the Court concluded that the export control regulation was an unconstitutional prior restraint on Professor Bernstein's speech.[148]

The Ninth Circuit decision was not a complete victory for Professor Bernstein and today's technologists for three reasons. First, the court here cautioned that its holding was narrow and applied only to this case with these sets of facts and emphasized that not all software is expressive. Second, it did not reach the question whether the government's regulation here was content neutral or content based. Third, *Bernstein* is no longer good law. Its complicated legal procedural history includes the three-judge panel's decision discussed earlier being withdrawn. The case was up for an *en banc* review by a panel of eleven justices.[149] However, before the rehearing took place, the government amended the regulations and eventually represented to the court that the regulations will not be enforced, rendering Professor Bernstein's lawsuit moot.[150] While this decision has no precedential value, it provides some insight into how other courts in the future might approach any possible regulations concerning encryption.

3. Standard of Review for Encryption Regulations

In *Karn v. U.S. Department of State*, the plaintiff claimed that the government violated his First and Fifth Amendment rights when it deemed a diskette containing cryptographic source code a defense commodity subjected to export-controls regulation while a book containing the same was not. The District of Columbia Federal District Court applied the traditional First Amendment analysis and found that the statute in question did not seek to regulate the content of speech. The government's interest in the export-control regulation was unrelated to the suppression of free expression. Because the regulation is content neutral, it is subjected to intermediate scrutiny. The court found that the government did have a substantial government's interest and that the regulation was

148 *Bernstein v. U.S. Dept. of Justice*, 176 F. 3d 1132, 1145 (Court of Appeals, 9th Circuit 1999).

149 The government requested an en banc review from the three justice panel's decision that affirmed the District Court's decision.

150 D. J. Bernstein, "Summary of Case Status, *Bernstein v. U.S. DOJ*," accessed November 19, 2016, http://cr.yp.to/export/status.html.

narrowly tailored.[151] The court here only assumed the source code is speech without deciding the constitutional question. Footnote 19 of the opinion explicitly made clear that "The Court makes no ruling as to whether source codes, without the comments, fall within the protection of the First Amendment. Source codes are merely a means of commanding a computer to perform a function."[152]

In contrast with *Karn* but similar to *Bernstein*, the Sixth Circuit Court found in *Junger v. Daley* that because source code has an expressive element, it is entitled to First Amendment protection.[153] However, upon reversing the District Court's finding on this issue of speech, the Sixth Circuit court did not perform any further constitutional analysis but remanded the case back to the District Court to decide whether the regulation on its face infringes on speech.[154] Again, similar to in *Bernstein*, because the government abandoned the policy of designation of encryption code as a munition and amended the regulation, the case became moot.

Despite the ardent wishes of the Electronic Frontier Foundation and other civil liberty groups, the issue of whether encryption source code is speech remains an open question. *Bernstein* is no longer good law and at least one court concluded that encryption code is not speech. Further, even if code is determined to be speech, bringing it into First Amendment coverage, its First Amendment protection is not absolute. Coverage is a threshold issue, while protection is the ultimate determination of the constitutionality of a particular legislation or government action. If an activity the government seeks to regulate is not speech under the First Amendment analysis, a court has to go no further. If it is speech that is covered under the First Amendment, a court will determine what level of protection it deserves, and whether the government's action infringing upon it has a compelling or substantial or important government interest, and whether the government's action is narrowly designed to achieve that interest.

---

151 *Karn v. U.S. Dept. of State*, 925 F. Supp. 1 (Dist. Court 1996).

152 Ibid., Footnote 19.

153 *Junger v. Daley*, 209 F. 3d 481, 485 (6th Cir., 2000).

154 Ibid.

4. Government Mandated Backdoor as Compelled Speech

The technology industry, cryptographers, and privacy advocacy groups have suggested that any government's action requiring the industry to design code to unlock encrypted devices is compelled speech in violation of the First Amendment.[155] Indeed, Apple raised this same argument with their support in its litigation against the FBI concerning the court order requiring it to design code to unlock the iPhone of one of the San Bernardino terrorists. Apple argued that computer code is speech and the magistrate's order that it write new code to unlock the subject's iPhone is the equivalent of compelling it to speak. In its briefing to the court, Apple argued:

> The government asks this Court to command Apple to write software that will neutralize safety features that Apple has built into the iPhone in response to consumer privacy concerns. The code must contain a unique identifier "so that [it] would only load and execute on the SUBJECT DEVICE," and it must be "'signed' cryptographically by Apple using its own proprietary encryption methods." This amounts to compelled speech and viewpoint discrimination in violation of the First Amendment.[156]

Apple's First Amendment argument failed for two reasons. First, Apple's claim that "[u]nder well-settled law, computer code is treated as speech within the meaning of the First Amendment"[157] is simply not true. As discussed previously, the Supreme Court has yet to opine on this issue. Furthermore, cases cited by Apple in support of this proposition such as *Bernstein v. Dept. of State* and *Junger v. Daley* are no longer good law and hold no precedential value.

Second, even assuming that code is determined to be speech, this determination is only a threshold matter triggering First Amendment analysis. It does not automatically afford Apple blanket First Amendment protection. It is likely that the court would find that code is content-neutral speech and therefore affords it less protection under the *Central Hudson* analysis discussed earlier. The government would only have to

---

[155] Andrew Crocker and Jamie Williams, "Deep Dive: Why Forcing Apple to Write and Sign Code Violates the First Amendment," March 3, 2016, Electronic Frontier Foundation, accessed February 3, 2017, https://www.eff.org/deeplinks/2016/03/deep-dive-why-forcing-apple-write-and-sign-code-violates-first-amendment.

[156] *In the matter of the Search of an iPhone*, 32.

[157] Ibid.

demonstrate an important government interest in fighting terrorism and pass the court's intermediate scrutiny. The Court has found many instances of government's compelled speech constitutional such as the surgeon general's warning on cigarettes, publicizing drugs' side effects, and labeling foods.[158] Perhaps Apple was only too aware that its First Amendment argument was not its strongest because the entire portion of the First Amendment argument was only three pages out of a 35-page brief. To date, this issue also remains open because the FBI withdrew its request for Apple's assistance and the order became moot.

B. THE FOURTH AMENDMENT

The Fourth Amendment provides "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[159]

It is axiomatic that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[160] More than with any other amendments in the Bill of Rights, the Fourth Amendment jurisprudence is an exercise in striking the balance between individual privacy and collective security. As Professor Orin Kerr wrote in *Applying the Fourth Amendment to the Internet,* "no sitting judge or justice today questions that the Fourth Amendment is a tool for imposing reasonable restrictions on police conduct."[161] Within the context of the going dark problem, the fundamental question to be explored is how Fourth Amendment jurisprudence applies to electronic surveillance. The answer turns on two legal doctrines: the Reasonable Expectation of Privacy doctrine and the Third Party doctrine.

---

[158] Charles M. English, "Compelled Speech and the First Amendment: Neutral Fact or Government Opinion?," *Legal Backgrounder, Washington Legal Foundation* 27, no. 1 (January 13, 2012), http:// www.wlf.org/upload/legalstudies/legalbackgrounder/1-13-12English_LegalBackgrounder.pdf.

[159] U.S. Constitution, Amendment IV.

[160] *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006).

[161] Orin S. Kerr, "Applying the Fourth Amendment to the Internet: A General Approach," *Stanford Law Review* 62, no. 4 (2009): 1005–50.

1. *Berger* and *Katz*, a Departure from the Reasonable Expectation of Privacy in Homes, Papers, and Effects

Essential to any discussion of how the Fourth Amendment applies to electronic surveillance is the reasonable expectation of privacy doctrine developed in two seminal wiretap cases decided in1967: *Berger v. New York* and *Katz v. United States*.

Up until the late 1960s, Fourth Amendment cases extended the protection from unreasonable searches and seizures only to three broad categories of property: homes, papers, and effects. "From the late nineteenth century until the 1960s, the Supreme Court deployed concepts linked to property law to interpret the scope and nature of the Fourth Amendment right to be free from unreasonable searches (and seizures of property)."[162]

Thus, when electronic surveillance technology became available and *Olmstead v. United States*, a case decided in 1928, presented the question of whether wiretapping constituted a search, the Court ruled it did not. Wiretapping did not trigger Fourth Amendment protection because the police did not enter the suspect's home to conduct such a search, and conversations were not papers and effects.[163]

Almost 40 years later, in 1967 the Supreme Court signaled a change in the physical space limitation of the Fourth Amendment protection in *Berger v. New York* by ruling that conversations were also protected under the Fourth Amendment. In *Berger*, the petitioner was convicted on two counts of conspiracy for bribing a New York Liquor Authority's official. His conviction was obtained through an extended and roving wiretap warrant executed by the police under authority of a state judge. New York criminal statute §813-a, authorizing this wiretap and eavesdropping upon a showing of "reasonable ground to believe that evidence of crime" might be obtained. The Supreme Court struck down the New York statute as unconstitutional on its face and reversed Berger's conviction.[164] In so doing, the Court determined that eavesdropping on conversations and electronic wiretaps constitute a "search" for purposes of the Fourth

---

[162] Morgan Cloud, "A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment," *Ohio State Journal of Criminal Law* 3 (2005): 33–73.

[163] *Olmstead v. United States*, 277 U.S. 438 (Supreme Court 1928)

[164] *Berger v. New York*, 388 U.S. 41(Supreme Court 1967).

Amendment, which meant oral statements are protected. "[A]uthorization of eavesdropping for a two-month period is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause."[165]

However, it was in *Katz v. U.S.*, decided a few months after *Berger*, that the Supreme Court clearly and unequivocally brought electronic surveillance into the Fourth Amendment protection. The central issue in *Katz* was whether a person has an "expectation of privacy," and not whether the government intrusion was physical or a violation of some property right.[166]

In *Katz*, the FBI placed listening devices on two phone booths that Charles Katz regularly used to place bets for interstate gamblers. Because there had been no physical intrusion into the phone booths, the government argued that there was no Fourth Amendment violation. Rejecting that argument and overturning *Olmstead*, the *Katz* Court ruled that the Fourth Amendment "protects people, not places." "Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[167] To make this determination, the court propounded a two-part test: whether the person has a "subjective expectation" of privacy and whether that expectation was "reasonable." Over the years, the reasonableness part of the test has been more of an emphasis for the Court than the subjective belief of an individual element.

2. Reasonable Expectation of Privacy in Cellphone Data

If *Berger* and *Katz* brought electronic surveillance into the Fourth Amendment protection, *Riley v. California* "brought the Fourth Amendment into the digital age" more than four decades later.[168] In a unanimous decision, the Supreme Court ruled that a

---

165 Ibid., 66.

166 *Katz v. United States*, 389 U.S. 347 (Supreme Court 1967).

167 Ibid., 359.

168 Marc Rotenberg and Alan Butler, "Symposium: In *Riley v. California*, a Unanimous Supreme Court Sets out Fourth Amendment for Digital Age," *SCOTUSblog*, June 26, 2014, http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/.

warrantless search of a cellphone's digital contents uncovered during an arrest constitutes an unreasonable search and therefore violates the Fourth Amendment.[169]

In *Riley*, the defendant was pulled over for an expired registration tag. During this routine traffic stop, the police learned that he was also driving with a suspended driver's license. His car was then impounded and a routine inventory search turned up firearms hidden under the hood of the car. He was then placed under arrest and searched. The police found a smartphone in his pants pocket. A detective later accessed the phone and found evidence including pictures and videos linking the defendant to gang activities and an earlier shooting. He was then charged and convicted in part based on the pictures and videos found on his phone. He appealed the conviction, arguing in part that the evidence on his cell phone was seized in violation of the Fourth Amendment and should have been suppressed. In opposition, the government argued that the search of the cell phone fell under the "search incident to arrest" exception to the warrant requirement and was, therefore, proper.[170] The search incident to arrest exception was widely accepted to protect two important government's interests: safety of the officers and destruction of evidence and was first recognized in *Chimel v. California*.[171]

The *Riley* court disagreed with the government and ruled that the interest in protecting the officer's safety was not present because cell phone data could not be used as a weapon. At the time of the arrest, the officer may physically examine the cell phone to ensure that it cannot be used as a weapon or to facilitate the arrestee's escape. However, the digital data stored on the cell phone could not be used as a weapon and therefore there was no exigent circumstance to justify searching digital data stored on an arrestee's cell phone without a warrant.[172]

Interestingly, the court also rejected the government's assertion that the searching of digital data incident to arrest was necessary based on its concerns that evidence would

---

169 *Riley v. California*, 134 S. Ct. 2473 (Supreme Court 2014).

170 Ibid., 2481.

171 *Chimel v. California*, 395 U.S. 752 (Supreme Court 1969)

172 *Riley v. California*, 134 S. Ct. 2473, 2485.

be destroyed by remote wiping or become unreachable by encryption when the cell phone was locked.[173] The Court found that there were targeted means for the government to address these concerns, such as disconnecting the phone from the network or placing it in a Faraday bag (sandwich bags made out of foil) to isolate it from radio waves. The Court theorized that in rare cases where an officer encounters a phone in an unlocked state, he or she may take steps to disable the auto-lock feature, similar to an officer securing a scene to preserve evidence.[174]

In balancing the government's heightened interests at a chaotic arresting scene with the arrestee's diminished privacy interest at the time of arrest, the Court still resolved in favor of the arrestee's privacy interest. This approach is due to the "qualitative" and "quantitative" difference between digital data on cell phone and traditional "papers and effects" recognized under the Fourth Amendment, according to the Court.[175] "Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[176] Chief Justice Roberts reasoned that because cell phones are ubiquitous and hold vast digital data that would implicate greater privacy concerns than a search of a home in a modern age, a warrant is required to access digital data, even when the phone is obtained from a search incident to arrest. He stated,

> The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.[177]

As far-reaching a decision as *Riley* is, it has two limitations relating to this thesis: First, the Court did not find the government's concerns over remote wiping and data encryption as persuasive reasons to apply the search incident to arrest exception to the

---

[173] Ibid., 2487–2488.

[174] Ibid.

[175] Ibid., 2489.

[176] Ibid.

[177] Ibid.

general requirement of a search warrant. The Court found remote wiping evidence presented by the government as "anecdotal"; and "data encryption is even further afield" than remote wiping.[178] It is important to note that this pronouncement only related to the government's argument for a search incident to arrest exception. The Court here did not pronounce that remote wiping and data encryption are not sufficiently prevalent in any other circumstances.

Second, in Footnote 1, the *Riley* Court explicitly explained that the holding only pertains to searches incident to arrest and that it does not implicate the question of "whether the collection or inspection of aggregated digital information amounts to a search under other circumstances."[179] The Riley decision assumes easily accessible data, at the time of arrest or after obtaining a warrant. Neither assumption can be made given the ubiquity of encryption today. Thus, whether encryption is sufficiently prevalent to warrant the Court's consideration of the government's interest in law enforcement or national security is still an open question.

The *Riley* decision was widely lauded as a sweeping victory for privacy rights and for bringing the Fourth Amendment into the 21st century because the Court recognized the ubiquity of cell phone use and that cell phone data is "qualitatively and "quantitatively" different from papers and effects that might be kept on a person.[180] Thus, *Riley* might very well be the key argument against any mandate to build backdoor into cellphone designs and operating systems. However, as will be discussed, if privacy rights advocates have *Riley* to support their position, law enforcement and intelligence agencies have the third-party doctrine to rebut the presumption that there is a reasonable expectation of privacy in all electronic data.

---

[178] Ibid., 2487.

[179] Ibid., Footnote 1.

[180] Adam Liptak, "Supreme Court Says Phones Can't Be Searched Without a Warrant," *New York Times*, June 25, 2014, http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html.

3. The Third-Party Doctrine

The third-party doctrine stands for the proposition that there is no expectation of privacy in electronic communications when the individuals knowingly shared the same with a third party, usually a service provider such as a bank (*U.S. v. Miller*), or a telephone company (*Smith v. Maryland*). In *U.S. v. Miller*, the defendant was an individual who does not have a legitimate "expectation of privacy" in checks and deposit slips since "they are not confidential communications but negotiated instruments" willingly disclosed to banks as a third party.[181] "The Fourth Amendment does not prohibit the government from obtaining information" that an individual willingly discloses to a third party.[182]

In *Smith v. Maryland*, the telephone company installed a pen register device on the defendant's phone line switch at the police's request. The pen register device recorded the phone numbers that defendant Smith dialed, one of which was of his robbery victim's home. The police then had reasonable suspicion to get a warrant to search Smith's home and he was eventually convicted based on the fruits of that search. The Supreme Court held that Smith had "no expectation of privacy [for] the phone numbers" [183] that he dialed as he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [Smith] assumed the risk that the company would reveal to police the numbers he dialed."[184]

The problem with the third-party doctrine is that the foundational cases of the doctrine were decided in the 1970s, before the advent of emails and cell phones. Writing in a concurring opinion in *U.S. v. Jones*, a 2012 case in which the Court ruled that attachment of a Global Positioning System (GPS) device on an individual car by the police constitutes an impermissible warrantless search and seizure, Justice Sotomayor

---

[181] *United States. v. Miller*, 425 U.S. 435, 442 (Supreme Court 1976).

[182] Ibid., 443.

[183] *Smith v. Maryland*, 442 U.S. 735, 742 (Supreme Court 1979).

[184] Ibid., 744.

signaled that the third-party doctrine might soon face its demise: "It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[185]

On the other hand, *Jones* marked the court's return to the physical trespass requirement in finding that by installing the GPS device on the target's vehicle, the government "physically occupied private property for the purpose of obtaining information."[186] Thus, the physical trespass in homes, papers, and effects test is still alive and well. Indeed, in response to Justice Sotomayor's suggestion that the physical trespass requirement is ill-suited for the digital age and reasonable expectation of privacy test should be the exclusive test, the majority explicitly disagreed. "[T]he *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test," the majority clarified.[187]

There is little doubt that the third-party doctrine will be revisited by the Supreme Court in the near future. The three cases challenging the NSA's bulk data collection programs implicating the third-party doctrine all have conflicting decisions among the circuit courts. The District Court of the Southern District of New York ruled in *ACLU v. Clapper* that the NSA's programs did not violate the Fourth Amendment based on the third-party doctrine in *Smith v. Maryland*.[188] Even the mass sweep of the data collection did not turn it into a Fourth Amendment search. Furthermore, the NSA's post-collection query of the telephone metadata does not constitute a search any more than the police's query of the FBI's fingerprint or DNA databases.[189]

While the District Court recognized the Supreme Court's reasoning in *U.S. v. Jones*, it emphasized that the Supreme Court did not overturn *Smith v. Maryland* and

---

185 *United States v. Jones,* 132 S. Ct. 945 (Supreme Court 2012).

186 Ibid., 949.

187 Ibid., 952.

188 *American Civil Liberties Union v. Clapper,* 959 F. Supp. 2d 724 (Dist. Court 2013).

189 Ibid. at 751–752.

therefore its precedent must be followed. On appeal, the Second Circuit affirmed the District Court's denial of the ACLU's application for a preliminary injunction but did not decide the constitutional issue.[190] Similarly, in a case brought in the Federal District Court of Idaho, *Smith v. Obama*, the Court applied the same rationale as in *ACLU v. Clapper* and dismissed the suit because *Smith v. Maryland* was still controlling.[191] On appeal, the Ninth Circuit dismissed the case as moot and did not reach the constitutional question at all.[192]

Contrast the last two cases with *Klayman v. Obama* in the District Court of the District of Columbia, also challenging the NSA's bulk metadata collection programs. Judge Richard Leon of the D.C. District Court found that the ruling in *Smith v. Maryland* cannot apply because NSA's bulk metadata collection programs cannot be analogized to the records of the pen register in *Smith v. Maryland*.[193] Judge Leon reasoned that the two cases are distinguishable because the NSA's programs collected records of millions of people unlike that of one defendant in *Smith v. Maryland*. Secondly, the NSA's programs lasted for several years, not several days as in Smith. Therefore, he concluded that the programs "likely" violated the Fourth Amendment and ordered a stay of the program.[194] However, upon appeal by the government, the second circuit vacated Judge Leon's order to stay. The case was also sent back to the district court for further proceeding on the issue of standing.[195]

As it is clear from the three cases challenging the NSA's programs discussed, prediction about the demise of the third-party doctrine might be premature. The Supreme Court is traditionally reticent about setting out bright line rule, especially when it involves technological advances. It took the Supreme Court almost 40 years to overturn

---

190 *American Civil Liberties Union v. Clapper*, 785 F. 3d 787 (Court of Appeals, 2nd Circuit 2015).

191 *Smith v. Obama*, 24 F. Supp. 3d 1005 (Dist. Court 2014).

192 *Smith v. Obama*, 816 F. 3d 1239 (Court of Appeals, 9th Circuit 2016).

193 *Klayman v. Obama*, 957 F. Supp. 2d 1 (Dist. Court 2013).

194 Ibid., 32–34.

195 *Obama v. Klayman*, 800 F. 3d 559 (Court of Appeals, Dist. of Columbia Circuit 2015).

Olmstead. It may take at least a decade of exponential technological innovations in the digital age for the Court to abandon the third-party doctrine.

4. National Security Exception

Another argument available to the government in enacting legislation or promulgating rules addressing the going dark problem is the national security exception to Fourth Amendment strictures. In his concurring opinion in *Katz*, Justice White argued for a national security exception to the warrant requirement due to the exigent nature in cases involving national security. He noted that

> wiretapping to protect the security of the Nation has been authorized by successive Presidents… We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.[196]

However, the *Katz* decision did not reach this question and expressly stated so in Footnote 23.[197]

In 1972, the Supreme Court unanimously extended the *Katz* ruling that a warrant is required for wiretaps in cases of national security in *U.S. v. U.S. District Court* (aka the *Keith* cases).[198] The *Keith* cases are instructive to our current discussion for two reasons: first, it was the first time that the Court weighed the national security interest against an individual's right of privacy after declining to do so in *Katz*. "Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the government attempts to act under so vague a concept as the power to protect 'domestic security.'"[199] Second, the Court expressed reservation that domestic electronic surveillance discretion should vest solely on the Executive Branch alone.

---

196 Ibid., 363–364.

197 Ibid. Footnote 23 stated: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."

198 "Smartphone Encryption and Public Safety," (2015).

199 *United States v. United States Dist. Court for Eastern Dist. of Mich*., 407 U.S.. 297, 314 (1972)

"These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[200]

In the *Keith* cases, the government charged three defendants with conspiring to destroy government property based on wiretaps obtained without a warrant. The government argued that the wiretaps were legal under the presidential power to protect national security. They supported this argument by citing to §2511(3) of Title III of the Omnibus Crime Control and Safe Streets Act, which Congress passed following *Katz* to govern domestic wiretapping in criminal investigations. Title III expressly stated that "nothing within the act limits the President's power to protect against the overthrow of the government" or to any "clear and present danger to the structure or existence of the government."[201]

The Court rejected this argument, ruling that §2511(3) is not an express grant of authority for the president to circumvent the warrant requirement of the Fourth Amendment.[202] However, the Court specifically limited its opinion to domestic threat against national security versus foreign threat against national security. The Court explicitly stated:

> This case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to the issues that may be involved with respect to activities of foreign powers or their agents. Nor does our decision rest on the language of § 2511(3) or any other section of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[203]

5. The Way Forward

Depending on the regulation being promulgated and the government's interest being advanced, encryption is not beyond the limits of government regulation. Applying

---

[200] Ibid., 316–317.

[201] Title III of the Omnibus Crime Control and Safe Streets Act of 1994, 18 U.S.C. §2511(3).

[202] *United States v. United States Dist. Court for Eastern Dist. of Mich.*, 407 U.S. 297, 303 (Sup. Ct. 1972).

[203] Ibid., 322. Note: In response to the Keith cases, Congress enacted The Foreign Intelligence Surveillance Act of 1978. It codified a regulatory regime for surveillance of a foreign threat against national security, thus addressing the gap left open by this case. Furthermore, in 1990 the Supreme Court ruled that the Fourth Amendment protection does not extend to non-U.S. persons in *Verdugo-Urquidez, supra*, and thereby agents of a foreign power.

the lessons from all the cases previously discussed, the government would do well to narrowly tailor any possible regulations to be content neutral, to meet strict Fourth Amendment warrant requirements and to clearly state the overriding national security interest in the age of terrorism and the complexity of investigating cybercrimes. Regulations addressing the going dark problem will have a better chance of passing constitutional challenges if they are supported by empirical data of how ubiquitous end-to-end encryption has significantly imperiled intelligence to combat terrorism and hindered cybercrime investigations and prosecutions. As the Supreme Court recognized in *Holder v. Humanitarian Law Project*, "[e]veryone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order."[204] The objective to keep in mind in reviewing proposed legislation or policy recommendations is not that the government's action will raise constitutional challenges but that it will pass constitutional review.

[204] *Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2724 (Supreme Court 2010).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. AMENDING CALEA TO MANDATE BACKDOOR ON COMMUNICATION DEVICES AS A POLICY SOLUTION

> Inconvenience and annoyance occasioned by more rigorous law enforcement are to be distinguished from realistic constitutional concerns about government intrusion.
>
> —Philip Bobbitt
> *Terror and Consent, The Wars for the Twenty First Century*

As discussed in the previous chapter on background and historical context, CALEA was enacted to address law enforcement's concerns over its diminishing capability to effectuate wiretap orders because the telecommunication industry in the early 1990s was undergoing a technical transformation from analog to digital switches. Because CALEA was adopted in 1994 before email and text messaging became commonplace, it originally only applied to telecommunications service providers. In 2006, the Federal Communications Commissions (FCC) extended CALEA requirements to broadband Internet access and Voice over Internet Protocol (VoIP) service providers. This extension still falls short of covering Internet communication service providers like Yahoo! or Internet platforms like WhatsApp.

With respect to the going dark problem, law enforcement officials have advocated that Congress amend CALEA to extend the mandate to Internet-based communications such as email and text messages provided by platforms like Gmail, Apple iMessages, and applications like WhatsApp. Such a policy, if adopted, would essentially mean that Internet-based service providers would have to engineer their hardware or software in such a way to enable them to respond to a lawfully obtained subpoena with readable text or to assist law enforcement with wiretaps despite the encryption features on their devices or services. The government calls this mandate a demand for "exceptional service." The technology industry calls this mandate a demand for a "backdoor."

A. THE PROPOSAL

While no specific legislation has been introduced, Manhattan District Attorney Cyrus Vance proposed in a November 2015 report (updated in 2016) titled *Smartphone Encryption and Public Safety* that Congress enact federal legislation requiring that "any smartphone manufactured, leased, or sold in the U.S. must be able to be unlocked, or its data accessed, by the operating system designer."[205] The specific language of the legislation would read as follows:

a) Capability Requirements

> A designer of an operating system used on smartphones or tablets manufactured, leased, or sold in the United States shall ensure that the data on any such smartphone or tablet using the designer's operating system is capable of being accessed by the designer in unencrypted form pursuant to a search warrant or other lawful authorization when the designer is in possession of the smartphone or tablet.

(b) Limitations

> 1. Design of system configurations
>
> This chapter does not authorize any law enforcement agency or officer:
>
> a. to require any specific design of operating systems to be adopted by any designer of operating systems; or
>
> b. to prohibit the adoption of any specific design of operating systems by any designer of operating systems.
>
> 2. Third-Party Encryption
>
> An operating system designer shall not be responsible for decrypting or ensuring the government's ability to decrypt, data

205 "Smartphone Encryption and Public Safety," Manhattan District Attorney's Office, November 2015. Updated November 2016, p. 32, https://assets.documentcloud.org/documents/3222483/White-Paper-2-0.pdf#page=3.

> encrypted by a user unless the encryption used was part of the design of the operating system.[206]

District Attorney Vance made clear that the proposal only addressed law enforcement's need to access data at rest on personal devices and took no position regarding data in transit. While there is no accurate way of quantifying how much of the going dark problem is due to encryption of data resting on devices, or due to encryption of data in transit between devices, it is clear that this proposal does not address the totality of the going dark problem.

B. APPLICATION

A federal mandate, most likely through an amendment of CALEA, would achieve the desired objective of giving law enforcement access to locked devices and encrypted applications. For example, had this mandate been in place at the time of the San Bernardino terrorists attack, Apple would not have been able to claim that it was unable to access Farook's iPhone, and the FBI would not have to engage in a public legal battle with Apple. Furthermore, the FBI would not have had to turn to the vulnerability market and pay just under $1 million for a technique to break into the iPhone.[207] Technical feasibility aside, this proposal will resolve the problem for law enforcement in accessing data at rest on a device in circumstances where the communication device is in their possession. Unfortunately, this proposal does not address law enforcement's inability to conduct wiretaps for real-time communications and therefore falls short of being a complete solution.

C. LEGAL AND ETHICAL CONSIDERATIONS

Any federal mandate imposing some limitations in manufacturers' encryption code may run into First Amendment challenges. Bringing the First Amendment analysis to the proposal of extending the CALEA mandate to smartphone manufacturers, I would argue that a *Bernstein* type of challenge does not apply here. This mandate is not prior

---

206 Ibid.

207 Mark Hosenball, "FBI Paid under $1 Million to Unlock San Bernardino iPhone: Sources," Reuters, May 4, 2016, http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032.

restraint of speech. The mandate does not require that the manufacturers obtain licensing under certain conditions and it does not impose some types of restrictions pertaining to their encryption code. It merely requires that manufacturers be able to provide law enforcement with access to encrypted devices that they designed. It simply imposes a legal obligation on smartphone manufacturers to cooperate with law enforcement the same way it did on telecommunications service providers in the early 1990s. The proposed amendment to CALEA here only extends the legal obligation on a new class of covered entities (i.e., smartphone manufacturers). It does not dictate a new obligation or how the manufacturers are to meet this obligation. Indeed, the Manhattan District Attorney's Office confirmed that it "does not propose any new technology, nor does it propose that governments hold a key to smartphones."[208]

Based on this analysis, extending a CALEA mandate to smartphone manufacturers as proposed by the Manhattan District Attorney's Office should not violate any constitutional protection.

D. LIKELIHOOD OF ADOPTION

Technologists have several objections to extending CALEA, most of which are in opposition to a mandated backdoor to encryption. "The most serious problem with CALEA, however, is that it has created a new class of vulnerabilities. By definition, a wiretap interface is a security hole because it allows an outside party to listen to what is normally a private conversation."[209] However, as District Attorney Vance argued in his 2015 report, his proposal is limited to addressing the need for law enforcement access to data at rest on a locked device. The potential risk for the government to hold the key to extract data on a locked device is far less than the potential risk for maintaining wiretapping capability for data in transit.

District Attorney Vance also argued in his 2015 report that Apple and Google have shown no evidence that the operating systems before iOS 8 for iPhones and

208 "Smartphone Encryption and Public Safety," 16, 2015.

209 Steven Bellovin et al., "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property* 12, no. 1, 19 (2014), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip.

Lollipop 5.0 for Android were any less secure for the users despite being without the default end-to-end encryption.[210] Furthermore, because the proposal at issue here pertains only to unlocking or extract data on smartphones, bad actors still need possession of the smartphone as well as the decryption key to do any harm. On the other hand, law enforcement will need to obtain a properly authorized search warrant before Apple and Google have to comply. Thus, personal privacy of ordinary citizens is protected.

Advocacy groups argue that this type of proposal puts human rights activists and political dissidents in undemocratic nations at risk in that repressive governments will require Apple and Google to violate activists and dissidents' privacy as well. This argument does not pass muster for two reasons. First, if Apple and Google chose to conduct business in countries with repressive laws and limited civil liberty, being asked to assist the government of that country with unlocking a dissident's locked smartphone would be neither the first, nor the only, nor the most unpalatable request that has been made of them—and to which they have acquiesced. In early 2017, Apple removed the *New York Times* app from its China App Store to keep the Chinese government happy.[211] Apple took this action only days before the *New York Times* published a series of articles about Apple receiving billions of dollars in subsidies from the Chinese government.[212] Thus, it would be disingenuous for manufacturers like Apple and Google to oppose this proposal on the basis of protecting human rights activists and political dissidents. Advocacy groups should lobby Apple and Google to not do business in countries with oppressive regimes altogether and/or not to give in to those governments' demands. They must also make Apple and Google to openly admit and begin to address the fact that cyber criminals, crime syndicates, sex trafficking, and child pornography rings also use the very same encryption technology to conduct business and evade justice.

---

210 "Smartphone Encryption and Public Safety," 14, 2015.

211 Sherisse Pham, "Apple Yanks New York Times Apps in China," CNNMoney, January 5, 2017, http://money.cnn.com/2017/01/05/technology/apple-nyt-china-app-store-remove/index.html.

212 David Gilbert, "Apple Removes New York Times from App Store to Keep Chinese Government Happy," VICE News, January 5, 2017, https://news.vice.com/story/apple-removes-new-york-times-from-app-store-to-keep-chinese-government-happy.

Second, a foreign government wanting information from an American company must pursue the matter under a Mutual Legal Assistance Treaty. The Executive Branch of the federal government will make the decision upon request. The other option is for the foreign government to seek information from an American company through a letter of rogatory, which is a formal request from a foreign court to a U.S. federal court for legal assistance, usually in service of process.[213] Compliance is not necessarily automatic. Vendors may choose to not comply with censorship like Google did in 2010 when it left China because it refused to censor its search results.[214] They may choose to resist a request for data from a foreign government that they find objectionable.

Lastly, Apple and Google have shown no evidence that repressive governments have requested them to unlock anyone's smartphones. As District Attorney Vance suggested, it is more conceivable that repressive regimes would compel the suspect directly to disclose the passcode rather than going through the lengthy legal process for smartphone manufacturers' assistance.[215]

If this proposal to amend CALEA is formally introduced as proposed legislation, the probability of its acceptance is high if the government does an effective public relations campaign educating the public about the counter-arguments to the technology industry and advocacy groups' arguments.

E. CONCLUSION

This proposal to extend CALEA mandate to smartphone manufacturers is constitutionally sound and has the likelihood of public acceptance. Yet, the limitation of this proposal only to data at rest leaves the other half of the going dark problem, namely data in transit, unaddressed. Without a policy solution addressing encryption of data in transit, law enforcement is unable to conduct wiretaps and access readable data, conversations, emails, texts in real time. This policy proposal falls short and leaves the government still in need of other solutions.

---

213 "Smartphone Encryption and Public Safety," 2015, 14.

214 Gilbert, "Apple Removes New York Times from App Store to Keep Chinese Government Happy."

215 "Smartphone Encryption and Public Safety," 2015, 27 endnote 66.

V. GOVERNMENT HACKING WITH A WARRANT AS A POLICY SOLUTION

> Law enforcement tactics must be allowed to advance with technological changes in order to prevent criminals from circumventing the justice system.
>
> —*U.S. v. Skinner,* 690 F.3d at 778 (6th Cir. 2012)

An approach that the cryptographers and technologists favor as a workaround solution to the going dark problem is lawful hacking. They argue that the government should increase the budgets dedicated to research and developing techniques to help law enforcement and intelligence agencies exploit already existing vulnerabilities[216] with an approved warrant. As described by some cryptographers in a seminal white paper, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*,

> Instead of building wiretapping capabilities into communications infrastructure and applications, government investigators can behave like the bad guys. That is, they can exploit the rich supply of security vulnerabilities already existing in virtually every operating system and application to obtain access to communications of the targets of wiretap orders.[217]

A. THE PROPOSAL

The *Urban Dictionary* defines hacking as "the gaining of access (wanted or unwanted) to a computer and viewing, copying, or creating data (leaving a trace) without the intention of destroying data or maliciously harming the computer."[218] Lawful hacking is hacking performed by law enforcement with an authorized court order. There are already relatively simple ways to hack into someone's data today. For example, any cell phone user's location, phone calls, and Internet browsing history are tracked by the

---

[216] A vulnerability is a weakness in the system that can be manipulated by someone to gain entry into the system. It can be a programming defect or a weak user's password. A zero-day vulnerability is one that has been discovered but not disclosed to the public or the vendor. A zero-day vulnerability is sold in vulnerabilities market.

[217] Ibid.

[218] *Urban Dictionary*, s.v. "Hacking," http://www.urbandictionary.com/define.php?term=hacking

mobile phone service provider. This information is readily available and searchable with a simple subpoena to the provider.[219] Even encrypted chats applications like WhatsApp requires account registration with a phone number. While the content of the chats is encrypted and unsearchable, the phone number is not and is susceptible to be turned over to law enforcement with a subpoena.[220] A group chat is only secure from wiretapping if everyone in the group activates end-to-end encryption. Assuming a lawful court order, a chat application service provider can add a new device to an account or a new participant without notifying the existing users, to allow law enforcement's access.[221]

However, the type of hack proposed by the technologists and cryptographers that is the subject of this chapter requires additional coding and is more complex. As explained in *Lawful Hacking*, computer systems are designed in "interdependent layers, each provides services to the one above it and requests services from the one below it."[222] The lowest layer is the hardware, CPU chips, hard drives, and USB ports. The "kernel" is the next layer and is a component of the system that communicates directly with external hardware like a network.[223] Each program in the system has strong separations so they cannot read or write from one another or from the network directly without permission. The kernel enforces this separation and also performs the task of writing or reading from the programs on their behalf.[224] The last layer is the "user level" or "application level." Such programs as web browsers, documents viewers, and mailers all run at the user level. The user may be an individual person or computerized processes called "daemons."[225]

---

219 Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World," *MIT Technology Review*, November 24, 2015, https://www.technologyreview.com/s/543896/6-ways-law-enforcement-can-track-terrorists-in-an-encrypted-world/.

220 Ibid.

221 Ibid.

222 Bellovin et al., "Lawful Hacking," 24.

223 Ibid., 25.

224 Ibid., 25.

225 Ibid., 26.

To penetrate a system and exploit its vulnerabilities, a hacker most often attacks at the user or application level. These attacks are usually done by infecting email attachments or by users downloading and executing booby-trapped programs. However, this level of exploit is not always useful for law enforcement in all cases as it is limited to intercepting email and reviewing transcript files of instant messaging programs. This limitation is due to other programs within the system being protected by the kernel.[226] Therefore, the second level of attack requiring a greater level of skills and expertise known as a "local privileges escalation" is needed to change device drivers and manipulate files.[227]

B. APPLICATION

The FBI had already been using hacking techniques to conduct surveillance. Documents obtained by the Electronic Frontier Foundation under the Freedom of Information Act revealed that the FBI has developed a proprietary technology called Computer and Internal Protocol Address Verifier (CIPAV), a type of malware. Once a CIPAV is installed on a target's computer, it can collect the Internet Protocol (IP) addresses'[228] list of programs running on that computer, language encoding, Uniform Resource Locator (URL) the computer was connected to, open communication ports, current user's login name, and other information that are associated to a Pen Register/Trap and Trace Order, among other capabilities.[229] The first reported case of the FBI's use of CIPAV was in 2007 in which the FBI identified a MySpace user who made

226 Ibid.

227 Ibid.

228 IP addresses are a unique identification number assigned to every computer being used on the Internet by the network administrator. It is traceable to a geographic location. https://www.lifewire.com/what-exactly-is-an-ip-address-2483347.

229 Jennifer Lynch, "New FBI Documents Provide Details on Government's Surveillance Spyware," Electronic Frontier Foundation, April 29, 2011, https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government.

bomb threats to a high school.[230] Another case was in 2013 in which the FBI used the same technique and a Rule 41 warrant to uncover two IP addresses in Tehran, Iran.[231]

As recently as 2014, the FBI used a remote search tool to investigate a child pornography website that operated on the TOR anonymity network and elaborated file encryption called Playpen. The FBI seized control of the website in 2014 but continued to operate it and installed CIPAV to the nearly 30,0000 members who logged onto the site.[232] Once installed (or infected) on the user's computer, CIPAV sent back to the FBI all requested information such as the user's IP and media access control (MAC) addresses.[233] With the IP and MAC addresses, law enforcement agents used traditional investigation techniques such as records checks, interviews, and physical search warrants to break the user's anonymity. This investigation led to more than 200 active prosecutions of active users of the child pornography website.[234]

There is no question that exploiting zero-day vulnerabilities also serves an important national security interest. For instance, "Olympic Games" is a codename for an operation in which the NSA attacked Iran's nuclear enrichment sites using four zero-day vulnerabilities. After damaging approximately 1,000 Iranian centrifuges, some experts argue that the cyber operation might very well be the force that drove the Iranians to the negotiation table.[235]

---

[230] Rule 41 of the Federal Rules of Criminal Procedures will be discussed extensively in the next section of this thesis.

[231] Richard R. Thompson II, "Digital Searches and Seizures: Overview of Rule 41 of the Rules of Criminal Procedures" (CRS Report No. R44547) (Washington, DC: Congressional Research Service, September 8, 2016), https://www.hsdl.org/?view&did=795598.

[232] Office of Public Affairs, "Colorado and Illinois Men Sentenced to Prison for Engaging in Child Exploitation Enterprise," U.S. Department of Justice, October 18, 2016, https://www.justice.gov/opa/pr/colorado-and-illinois-men-sentenced-prison-engaging-child-exploitation-enterprise.

[233] A MAC address or Media Access Control address is a unique identifier assigned to network devices by the manufacturer, such as computer type and model. It can usually be referred to as a physical or hardware address that was hardwired into the device (http://whatismyipaddress.com/mac-address).

[234] Leslie Caldwell, "Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation," U.S. Department of Justice, November 21, 2016, https://www.justice.gov/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation.

[235] David E. Sanger, "Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say," *New York Times*, April 12, 2014, https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html.

C. LEGAL AND ETHICAL IMPLICATIONS

Although this policy advocates that law enforcement will perform hacking surreptitiously, it will only be done only after being fully authorized by a search warrant issued by a court of competent authority. This section discusses whether the policy and practice of legally authorized hacking are contrary to constitutional standards and comports with our national values and ethics. Because a properly obtained warrant meeting all the Fourth Amendment requirements is the starting point of this policy, this section will not discuss issues of probable cause or reasonable expectation of privacy in an IP address or in a computer.

If the U.S. government were to formally adopt lawful hacking as a policy, law enforcement must obtain a warrant before commencing any hacking attempts. Multiple warrants may be required for hacks that are more complex. Multiple warrants might also be required in cases in which additional traditional investigation techniques such as a physical search of the device or the home of the suspect are needed. For example, in the Playpen cases, the FBI first obtained a search warrant to install the CIPAV malware on a suspect's computer. Once the CIPAV collected the suspect's IP and MAC addresses and the FBI used them to break the suspect's anonymity, they then obtained a second search warrant to monitor the suspect's communications.[236]

Criminal investigations and prosecutions in the federal courts are governed by the Federal Rules of Criminal Procedure. Rule 41, first codified in 1917, specifically governs the requirements and conditions under which a search warrant may be issued. Under Rule 41, the government is required to apply for a warrant in the same jurisdiction where a property to be searched is located. However, in the age of encryption and ubiquity of anonymizing browsers such as TOR, investigators often do not know where the suspect is located at the time they seek a warrant to begin the initial hacking to break the suspect's anonymity. Courts in some federal jurisdictions have excluded evidence in a number of Playpen prosecutions due to this procedural defect.[237]

---

[236] Bellovin et al., "Lawful Hacking," 31.

[237] Caldwell, "Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation."

For these reasons, the Justice Department proposed a change to Rule 41 to allow law enforcement to obtain warrants to remotely search computers without having to specify the geographic location of the target. The amendments were first proposed in 2013 and were subjected to lengthy periods of public comments and a deliberative process by the federal judiciary. The U.S. Supreme Court finally adopted it on April 28, 2016. Opponents to the change insist that the new rule will provide the government a way to bypass the Fourth Amendment requirement of specificity, an important safeguard against government's authority to conduct electronic surveillance. In support of the rule change, Justice Department spokesman, Peter Carr, argued that this is an important evolution of the Criminal Rules: "Criminals now have ready access to sophisticated anonymizing technologies to conceal their identity while they engage in crime over the Internet, and the use of remote searches is often the only mechanism available to law enforcement to identify and apprehend them." The Justice Department also argued that the rule change does not enlarge the government's power into searches that have traditionally been prohibited by law. The government must still abide and satisfy the Fourth Amendment requirements.

Indeed, the committee note on the amendment shows that "[t]he amendment would eliminate the burden of attempting to secure multiple warrants in numerous districts, and allow a single judge to oversee the investigation."[238] The committee also made clear that the amendment does not address the constitutional question and leaves the specificity required by the Fourth Amendment to the development of case law.[239] Furthermore, the amended venue provisions only identify the appropriate court to consider the warrant applications, not authorize the warrants automatically.[240] The Supreme Court approved and the new change went into effect in early December 2016. This change means that law enforcement may apply for a search warrant with any federal

---

238 "Rule 41. Search and Seizure," Federal Rules of Criminal Procedure, accessed December 13, 2016, https://www.federalrulesofcriminalprocedure.org/title-viii/rule-41-search-and-seizure/.

239 Ibid.

240 Leslie Caldwell, "Additional Considerations Regarding the Proposed Amendments to the Federal Rules of Criminal Procedure," U.S. Department of Justice, (November 28, 2016), https://www.justice.gov/opa/blog/additional-considerations-regarding-proposed-amendments-federal-rules-criminal-procedure.

magistrate to remotely access, search, seize and copy data on any computer anywhere in the world that used technological means to obscure its location, or when a computer is swept up in a "botnet" without providing notice to the users being searched. [241]

With the change in Rule 41, assuming law enforcement meets Fourth Amendment requirements when applying for a search warrant that will be evaluated by a court of competent jurisdiction on a case-by-case basis, the policy of promoting lawful hacking as a solution to the going dark problem does not have any constitutional deficiency. With respect to ethical issues associated with lawful hacking, policymakers will have to evaluate trade-offs and decide on lesser-evil options. When the FBI successfully wrestled control of the Playpen website on the TOR network, instead of immediately shutting it down and arguably preventing additional child pornography trafficking on that site, they continued to operate it to bait others who visited the site, installed CIPAV on the visitors' computers, and eventually obtained evidence to arrest and prosecute hundreds of child pornographers.

Another ethical dilemma is whether law enforcement has an obligation to report vulnerabilities to the vendor for immediate patching, regardless if they uncovered the vulnerabilities in the system themselves, or purchased it on the vulnerabilities market. Retaining vulnerabilities assists the government in conducting investigations and surveillance for law enforcement and national security purposes but leaves millions of ordinary Internet users vulnerable to attacks by criminal hackers. On the other hand, disclosing the vulnerabilities for immediate patching by the vendor forecloses the possibility that they can be used later to lawfully hack into suspect's systems to further law enforcement purposes.

The dilemma is not merely theoretical. When the FBI purchased the zero-day vulnerability to unlock the iPhone that belonged to one of the San Bernardino terrorists, it did not share it with Apple, claiming it did not own the technical information

[241] A botnet is a number of computers that are co-opted to send spam or virus to other computers without their owners being aware of it. It is also known as a "zombie army." http://searchsecurity.techtarget.com/definition/botnet.

underpinning the tool.[242] The NSA was believed to have known about a flaw in the way that many websites sent sensitive information and had been exploiting it for two years before it was uncovered by researchers in April 2014.[243] This vulnerability, dubbed the "Heartbleed" bug, might have been the biggest security breach in the history of the Internet, but the NSA reportedly opted to keep it a secret to pursue its national security interest. While the NSA vigorously denied prior knowledge of Heartbleed, the Obama administration disclosed publicly for the first time that there was a process by which competing interests in the offensive and defensive use of vulnerabilities are considered in light of the national security and law enforcement needs. The White House emphasized that the process is heavily biased toward disclosing vulnerabilities except in cases of a "clear national security or law enforcement need."[244]

The Vulnerability Equity Process (VEP) first originated in 2008 and 2009 from a working group and consisted of members of the National Security Council, Central Intelligence Agency, Defense Intelligence Agency, Justice Department, Federal Bureau of Investigation, Department of Defense, Department of State, Department of Energy, Department of Homeland Security, and led by the Office of the Director of National Intelligence following recommendations from President George W. Bush's National Security Policy Directive 54. The group established a process by which the government's response to knowledge of a specific vulnerability is taken in consideration of the offensive and defensive needs of the national security mission.[245] The VEP ensures that decisions surrounding an uncovered zero-day vulnerability are made expeditiously and with full consideration of all the equities' interests involved, including those of the

---

[242] Katie Bo Williams, "FBI Shares Apple Vulnerability through Controversial Review," The Hill, April 26, 2016, http://thehill.com/policy/cybersecurity/277845-fbi-used-controversial-wh-review-to-tell-apple-about-older-security-hole.

[243] Michael Riley, "NSA Said to Have Used Heartbleed Bug, Exposing Consumers," *Bloomberg.com*, April 11, 2014, https://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.

[244] Sanger, "Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say."

[245] Ari Schwartz and Rob Knake, "Government's Role in Vulnerabilities Disclosure: Creating a Permanent and Accountable Vulnerability Equity Process" The Cyber Security Project, Belfer Center for Science and Security Affairs, Harvard Kennedy School, 2016, 4, http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf.

government organizations tasked with conducting intelligence, military operations, and critical infrastructure protection.[246]

Under this process, an agency that gains possession of a zero-day vulnerability must notify the executive secretary of the Vulnerability Equity Process Committee, who will then disseminate the vulnerability to the subject matter experts (SME) designated by each agency. Ultimately, the Executive Review Board makes the decision whether to disclose a vulnerability or to retain it and disclose it at a later date.[247] According to the government, the board discloses approximately 91 percent of newly discovered vulnerabilities and the remaining 9 percent are retained for national security or law enforcement use.[248] However, a great deal of the VEP remains classified, including the memberships, the decision-making process, and the review process.[249]

Criticisms surrounding the government's discovery, possible retention, and subsequent exploitation of zero-day vulnerabilities take two major veins. The first recognizes the important national security and law enforcement interests and takes a more realistic approach in advocating for more transparency in the VEP.[250] Proposals for more transparency include formalizing the VEP through an Executive Order, declassifying the criteria used to determine when a vulnerability will be retained due to national and law enforcement's needs and when a vulnerability will be disclosed to a vendor for patching, requiring that the executive secretary issue an annual report similar to the wiretaps report the Administrative Office of the Courts is required to make.[251]

The second group of critics starts with the premise that unpatched vulnerabilities are inherently destabilizing especially for the United States because of its electronic

---

246 Ibid., 5.

247 Ibid.

248 Susan Hennessey, "Vulnerabilities Equities Reform That Makes Everyone (And No One) Happy," Lawfare, July 8, 2016, https://www.lawfareblog.com/vulnerabilities-equities-reform-makes-everyone-and-no-one-happy.

249 Ibid.

250 Ibid.

251 Schwartz and Knake, "Government's Role in Vulnerabilities Disclosure: Creating a Permanent and Accountable Vulnerability Equity Process," 14–16.

infrastructure, heavy reliance on the Internet, and its wealth. While they recognize that other countries hostile to the United States also stockpile vulnerabilities,[252] this group argues that disclosing vulnerabilities as soon as they are found is not disarmament. By doing so, "[w]e also regain the moral authority to negotiate any broad international reductions in cyber-weapons; and we can decide not to use them even if others do."[253]

Fortunately, there is also a middle ground on this issue. Except in extreme cases, vulnerabilities discovered by the government may be disclosed immediately without compromising law enforcement's ability to use them for several reasons. According to the authors of *Lawful Hacking*, it takes time for the vendor to engineer a patch. Once it is engineered, such a security patch is not always immediately released to the public for an update. Typically, a vendor releases security patching on a schedule, usually once a month or once every six weeks.[254] Once a security patch is released, it is not always updated immediately by the users. The average lifespan for a zero-day vulnerability is ten months, according to empirical research.[255] Thus, except in rare cases, the government should be able to exploit the vulnerability for wiretap before it is barred by the vendor's security patches.

D. LIKELIHOOD OF ADOPTION

Lawful hacking as a proposed solution to the going dark problem has a higher potential for acceptability by policymakers and the public than an extension of CALEA in at least three ways. First, it gives law enforcement the tools to conduct investigations and surveillance specifically targeting bad guys without making the Internet more

---

[252] Stockpiling vulnerabilities is a practice by which usually nation states but not always hoard zero-day vulnerabilities for surveillance, espionage and theft of data, intelligence, and intellectual property. In cyber warfare, zero-day vulnerabilities are cyber weapons. In August 2016, a group self-identified as "Shadow Brokers" dumped 300 megabytes of the NSA data revealing that it has been stockpiling vulnerabilities as cyber weapons. Bruce Schneier, "The NSA Is Hoarding Vulnerabilities," Schneier on Security, August 26, 2016, https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html.

[253] Bruce Schneier, "Disclosing vs. Hoarding Vulnerabilities," Schneier on Security, May 22, 2014, https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html.

[254] Bellovin et al., "Lawful Hacking," 54.

[255] Leyla Bilge and Tudor Dumitras, "Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World," *Proc. 2012 ACM Conf. on Computer & Comm. Security* 833, 834 (2012).

insecure for the rest of law-abiding citizens. From the technology industry's perspective, exploiting existing vulnerabilities are preferable to mandating backdoor access for the government.[256] President Obama's Review Group on Intelligence and Communications Technology recommended that the US government fully support and encourage the use of encryption to better protect data (Recommendation #29) but at the same time recognized the need to use zero-day vulnerabilities for high priority intelligence collection (Recommendation #30).[257]

Even the Electronic Frontier Foundation (EFF), whose primary mission is to protect individual privacy rights on the Internet, accepts lawful hacking as a preferable alternative to mandating backdoor. "If the FBI obtains a probable cause-based court order before installing tools like CIPAV, complies with the minimization requirements in federal wiretapping law by limiting the time and scope of surveillance, and removes the device once surveillance concludes, the use of these types of targeted tools for Internet surveillance would be a much more narrowly tailored solution to the FBI's purported problems than the proposal to undermine every Internet user's privacy and security by expanding CALEA."[258]

Second, it brings hacking, an activity that used to be in the shadows and carried negative connotations into the public realm with legal oversight and for the benefit of the public. Some might argue that the proposal for lawful hacking has a whiff of dirty play about it,[259] but I disagree. By having a formalized policy that the government is actively pursuing vulnerabilities exploits for national security and law enforcement purposes, it brings the technique from being normally associated with the shadowy world of criminals and black hat hackers into a systematic and legally sanctioned approach.

Lawful hacking is nothing more than wiretapping in the digital age. The Seventh Circuit Court once opined in a case in which the FBI created fictitious cases to uncover

---

256 Jaffer and Rosenthal, "Decrypting Our Security," 254

257 Clarke et al., "Liberty and Security in a Changing World," 36–37.

258 "The Playpen Cases: Mass Hacking by U.S. Law Enforcement," Electronic Frontier Foundation, August 15, 2016, https://www.eff.org/cases/playpen-cases-mass-hacking-us-law-enforcement.

259 Bellovin et al., "Lawful Hacking,"64.

corruptions in the legal system: "In the pursuit of crime the Government is not confined to behavior suitable for the drawing room. It may use decoys . . . and provide the essential tools of the offense . . . The creation of opportunities for crime is nasty but necessary business."[260] With clear legislative limitations at the outset and judicial oversight on a case by case basis of each search warrant applications, lawful hacking is the technical solution to bridge the policy gap created by ubiquitous end to end encryption.

Third, lawful hacking is an elegant middle-ground solution to the going dark problem because it strikes the right balance between privacy and security. In requiring that law enforcement obtains a lawful warrant meeting all the Fourth Amendment requirements, privacy concerns are addressed. In passing legislation publicly and formally sanctioning hacking with a warrant, policymakers are legitimizing this effective law enforcement tool and endorsing evidence gathered through this tool as admissible evidence in any prosecution.

Fourth, lawful hacking is also an effective tool because it addresses both data at rest and data in transit whereas amending CALEA only addresses data at rest on a device. Furthermore, with this solution, law enforcement does not have the concern that the hardened criminals and sophisticated terrorists are beyond law enforcement's reach. Those that are beyond law enforcement's reach are so because of other factors such as the ticking time bomb scenarios, and not because the proposed legislation drove them further into the Dark Net or stronger encryption.

E. CONCLUSION

It is clear from the Playpen prosecutions and from the NSA's success in operation Olympic Games that the government has already been exploiting vulnerabilities to accomplish its national security and law enforcement missions, whether by discovering vulnerabilities on their own or by purchasing vulnerabilities on the vulnerability market. It is also clear that they have been effective. Thus, lawful hacking can be an effective and legitimate tool, in addition to available data sources such as metadata on cloud servers and the Internet of Things, to aid law enforcement in working around end-to-end encryption.

[260] *United States v. Murphy*, 768 F. 2d., 1518, 1524 (7th Cir. 1985).

VI. RECOMMENDATIONS AND CONCLUSION

> If we are to protect our civil rights and civil liberties against [the threat posed by global terrorist network], the aggressive use of informants, surveillance, wiretaps, searches, interrogations, and even group-based profiling must be measured not only against the liberties these practices constrict, but also with respect to the liberties they may protect."
>
> —Philip Bobbitt
> *Terror and Consent, The Wars for the Twenty-First Century*

I started this thesis with the presumption that this going dark problem is representative of the tension between individual privacy and public safety. Specifically, it is about keeping our data and communications safe from thieves and eavesdroppers versus keeping the public physically safe from criminals and terrorists. Yet, while FBI Director Comey and other government officials publicly and repeatedly acknowledge that encryption is valuable, there has been no acknowledgment from the technologists and privacy advocates that public safety is served by law enforcement and intelligence agencies being able to access information and evidence pursuant to a properly executed court order.

The most technologists had done in this regard is stating that they "take no issue with law enforcement's desire to execute lawful surveillance orders when they meet the requirement of human rights and the rule of law."[261] This simply means: "I see *you* have a problem," whereas the first step in resolving any dispute is an acknowledgment that "*we* have a problem." One has to recognize and start with the assumption that the solution for the going dark problem will require a risk and cost balancing approach and tradeoffs by both sides. For this reason, I agree with Director Comey in his attempts to speak out about this problem in both of those terms: universal encryption is valuable but there is a cost to public safety and the constitutional rule of law. In a speech given at the Brookings Institution in July 2015, Director Comey stated:

[261] Abelson, et al., "Keys Under Doormats" (2015), p. 1.

> When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We 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. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence.[262]

This discussion of the cost to public safety may seem theoretical at this time because the FBI has yet to gather, much less present, any details regarding the number of cases in which end-to-end encryption had frustrated their investigations. However, whatever that number might be, it is undeniable that end-to-end encryption presents a problem for law enforcement and intelligence agencies.

Fair-minded people may agree or disagree about whether the going dark problem is big or small or a problem at all, or if it deserves a national debate and legislative mandate, but let us agree that there is a downside to end-to-end encryption. It hinders law enforcement from executing a lawful court warrant. It allows private corporations to thumb its nose at court orders while individual private citizens are not able to do so without facing legal consequences. Hoping to facilitate a fair-minded and healthy discussion, Director Comey stated in an article for *Lawfare* on July 6, 2015:

> My job is to try to keep people safe. In universal strong encryption, I see something that is with us already and growing every day that will inexorably affect my ability to do that job. It may be that, as a people, we decide the benefits here outweigh the costs and that there is no sensible, technically feasible way to optimize privacy and safety in this particular context, or that public safety folks will be able to do their job well enough in the world of universal strong encryption. Those are decisions American should make, but I think part of my job is to make sure the debate is informed by a reasonable understanding of the costs.[263]

However, the only public safety that technologists seem to care about is the security of the Internet. One of the *Keys Under Doormats* authors, Bruce Schneier's

---

[262] Comey, "Going Dark" (2014).

[263] Comey, *Lawfare* (2015).

position on this issue can be summed up by a line in his 2015 book *Data and Goliath*: "Security has to come first, eavesdropping second." For him, cybersecurity is paramount because law enforcement may resort to an array of investigative tools at their disposal to get the data they need without weakening security for everyone.[264] This type of argument does not advance the discussion toward resolution. It does quite the opposite. Furthermore, technologists speak of this problem with the assumption that encryption is the end all and be all of keeping cyber infrastructures and communications safe, and creating secure exceptional access is not only undesirable, it is *not* technically feasible.[265] Ross Anderson, professor of security engineering at the University of Cambridge and another author of *Keys Under Doormats*, wrote: "The government's proposals for exceptional access are wrong in principle and unworkable in practice."[266]

Perhaps we can start with agreeing that there is no absolute security, in cyberspace or anywhere else. Even with encryption, there are still risks of compromised data from hackers or hostile nation-states because of the human factor. As the President's Council of Advisors on Science and Technology found: compromises of data can and will occur by being stolen or mistakenly shared. Even when data is encrypted, a hacker can attack the machine and steal data the moment before it is encrypted and sent, or after it is decrypted by the receivers/readers.[267] Thus, all can agree that Internet security is always a managed risk endeavor.

Then, why speak of the going dark problem and the attendant public safety concerns in zero-sum terms like Schneier did in *Data and Goliath*? For example, in a statement to the *New York Times* on September 27, 2010, FBI General Counsel Valerie Caproni said: "No one should be promising their customers that they will thumb their nose at a U.S. court order. They can promise strong encryption. They just need to figure

---

264 Bruce Schneier, *Data and Goliath* (New York: W.W. Norton, 2015), 182.

265 Abelson, et al., "Keys Under Doormats," 1, 7; Nicole Perlroth "Security Experts Oppose Government Access to Encrypted Communication," *New York Times*, July 7, 2015.

266 Perlroth, "Security Experts Oppose Government Access to Encrypted Communication."

267 President's Council of Advisors on Science and Technology (2014)

out how they can provide us plain text."[268] To this statement, Schneier responded: "Translation: you can't actually provide security for your customers."[269] If the government is wrong for overstating the going dark problem, then technologists are equally wrong in framing this problem as a zero-sum proposition.

Technologists are also fond of referring back to the Crypto Wars of the 1990s to reiterate that their predictions regarding the security of the Internet and how the exponential growth of the Internet was aided by encryption and unfettered access to encryption technologies. They wanted to apply the lessons of the first Crypto Wars to today by claiming that nothing has changed.[270] In *Key Under the Doormats,* the entire section of "What has changed and what remains the same since 1990s?" was devoted to technological changes and the proliferation of Internet commerce.

> Today, the fundamental technical importance of strong cryptography and the difficulties inherent in limiting its use to meet law enforcement purposes remain the same. What has changed is that the scale and scope of systems dependent on strong encryption are far greater, and our society is far more reliant on far-flung digital networks that are under daily attack.[271]

And there was more of the same throughout the paper. Not once was the threat against national security in the age of terrorism post-9/11 mentioned. Daniel Kehl, Andi Wilson and Kevin Bankston of the Open Technology Institute also expressed the same sentiment in their paper *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s*: "We already had a robust public debate that resolved this dispute, and nothing has changed since the 1990s that would cast doubt on the policy conclusions we reached then; indeed, the post-war period has only reinforced those conclusions."[272]

---

[268] Charlie Savage, "Surveillance Court Rules that NSA Can Resume Bulk Data Collection," *New York Times*, June 30, 2015. https://www.nytimes.com/2015/07/01/us/politics/fisa-surveillance-court-rules-nsa-can-resume-bulk-data-collection.html.

[269] Schneier, *Data, and Goliath*, (2015), 83.

[270] Abelson, et al., "Keys Under Doormats"; Kehl, "Encryption 101"; Kevin Bankston, "It's Time to End the Debate on Encryption Backdoors," *Just Security*, July 7, 2015.

[271] Ibid., 8.

[272] Kehl, et al., "Doomed to Repeat History," 21.

While I agree that nothing has changed that would weaken the Internet security imperative, lessons from the intelligence failures of 9/11 and the proliferation of terrorist recruitment on the Internet cannot be easily dismissed. Technology and its wonderful advances do not exist in a vacuum. As ordinary citizens and U.S. enterprises are enjoying the security and privacy of end-to-end encryption, so are the criminals and the terrorists. *Inspire* magazine, known to be an al Qaeda propaganda publication, directs its reader to contact them via encrypted platforms: "We strongly encourage everyone to use the Asrar el Mujahideen program to get in touch with us…to avoid detections by intelligence agencies," and provided its public key for encrypted emails.[273]

As Deputy Attorney General Yates testified before the Senate Judiciary Committee in 2015, it is also on strongly encrypted apps and devices that ISIL is actively recruiting Western Europeans and Americans to travel to Syria to join their fight, or worse yet, commit lone-wolf killings of specific targets right here in the United States.[274] The U.S. House of Representative Homeland Security Committee's bipartisan Task Force on Combating Terrorism and Foreign Fighters reported in September 2015:

> In almost 80 percent of cases, we found examples of U.S. foreign fighter aspirants downloading extremist propaganda, promoting it online, or engaging with other extremists on social media. Some communicated with ISIS fighters in Syria using secure messaging apps like *Surespot* or posed questions to overseas jihadists via the anonymous website *Ask.fm*; others promoted jihadist content across multiple platforms.[275]

Therefore, I assert that a lot has changed. More than ever, the United States must ensure that its intelligence, counter-terrorism, and law enforcement agencies are able to perform their jobs, not at the sacrifice of individual liberty but with all the constitutional safeguards. Encryption is valuable, but in cases where the government is able to identify a target with reasonable suspicion and meet all the Fourth Amendment requirements, that

---

273 "How to Communicate with Us," *Inspire*, 1434, no. 11 (Spring 2013), https://azelin.files.wordpress.com/2013/05/inspire-magazine-issue-11.pdf.

274 Written statement of Sally Quillian Yates.

275 "Final Report of the Task Force On Combating Terrorist And Foreign Fighter Travel," Homeland Security Committee, September 2015, https://homeland.house.gov/wp-content/uploads/2015/09/TaskForceFinalReport.pdf.

surveillance target should not be able to enjoy the benefits of strong encryption to evade detection, capture, and justice.

Some readers may disagree with my assertion that technologists do not recognize national security as a sufficiently valuable interest in this going dark debate to engender a compromise. They may point to numerous discussions in Schneier's *Data and Goliath* to support the notion that technologists do recognize that 9/11 greatly affected the work of intelligence and law enforcement. Readers may simply assert that there are a number of tools available for law enforcement to use without compromising the security of the Internet. However, I maintain that a closer reading of *Data and Goliath* would reveal that (1) Mr. Schneier's main targets of contempt and mistrust (rightly or wrongly) were the National Security Agency and its many mass surveillance programs against Communists during World War I, civil rights leaders and Vietnam War protesters.[276]

Yet here, the going dark problem is one of *targeted* surveillance *authorized* by a court warrant that met all the constitutional safeguards of the Fourth Amendment. It is on this point that the government and technologies are furthest apart and seem to be talking past each other. Strong encryption is a reality and a certain future. Both sides need to move forward toward cooperation on new tools that the government may use for lawful purposes without mandating a backdoor to encryption.

To be fair, Schneier did call for new ideas, tools, and techniques to help governments collect data for legitimate national security and law enforcement purposes. Perhaps he did recognize that should this impasse continue, the government might propose legislations or technologies and impose them on the technology industry without its input. He did recognize that "[i]f we want organizations like the NSA to protect our privacy, we're going to have to give them new ways to perform their intelligence jobs."[277] However, as late as the end of 2015, it is unclear what initiative Schneier took to implement this noble call.

---

[276] Schneier, *Data, and Goliath,* 102.

[277] Ibid., 220.

A. RECOMMENDATIONS

My recommendations concerning the most effective middle-ground solution to the going dark problem include legislative action and a public education campaign.

1. Legislative Action

I recommend that policymakers adopt legislative actions to legalize and thereby legitimize hacking by law enforcement in limited cases as a middle-ground solution. As previously stated, government hacking with a lawful warrant satisfying Fourth Amendment requirements is preferable to mandating exceptional access for several reasons. It strikes the right balance between public safety and private liberty by giving law enforcement the tool to investigate and prosecute crimes in the digital age while still safeguarding the security of the Internet and individual privacy with a required search warrant. Unlike extending the CALEA-like mandate to require that device manufacturers assist law enforcement in unlocking smartphones, lawful hacking as a solution addresses the encryption problem for both data at rest and data in transit. However, to address concerns of government overreach and to win broad public support for the proposal, I also recommend the following limitations and minimizing procedures adopting Professor Daniel Solove's prescription: "Government investigations must be minimized to prevent sweeping dragnet searches. Investigations must be particularized to specific individuals suspected of criminal wrongdoing. And there must be meaningful oversight over law enforcement activities."[278]

a. Minimizing Procedures

I propose the following minimizing procedures which mirror that of the Federal Wiretap Act:

1. A warrant granted under this proposed legislative mandate must only be issued in connection with an investigation or prosecution of crimes enumerated in the federal statute authorizing judges to approve wiretaps, oral or electronic communication interceptions, 18 U.S.C. §2516 (Title 18).

[278] Daniel Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference," *Fordham Law Review* 74, no. 2 (2005): 747, 775.

2. A warrant application under this proposed legislative mandate must clearly include a sworn statement as to whether other investigative methods have been tried or not and why other methods have failed or deemed to be likely unsuccessful or too dangerous. This requirement is similar to the mitigation requirement of 18 U.S.C. §2518 (Title III of the Omnibus Crime Control and Safe Street Act.)

3. A warrant order must mirror Section 2518(4) of Title III which states: "Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify— (a) the identity of the person, if known, whose communications are to be intercepted; …(c) c) a particular description of the type of communication sought to be intercepted."[279] Additionally, the order must set clear limitations regarding time-span for collection and items to be collected and their use on any order authorizing hacking.

b. Transparency Requirement

Similar to the requirement under Title III that the Administrative Office (AO) of the Court compile a Wiretap Report, a Vulnerabilities Exploits Report should also be required on an annual basis. The AO should be reporting on the number of exploits performed each year, the duration of the exploits, whether the vulnerabilities were later reported and how long before they were reported.

c. Broader Applicability

Law enforcement agencies are not monolithic. A rural county's law enforcement agency will not have the same budget and technical expertise as the FBI does to conduct authorized hacking. If this proposed policy is to be effective in providing the tool for law enforcement to get around the going dark problem, policymakers need to be mindful of the disparity in resources among various law enforcement agencies. Therefore, I recommend that Congress increase the FBI's budget to implement this policy and direct the FBI to establish a lab specifically dedicated to assist local law enforcement agencies with their technical expertise.

It is necessary to ensure that the Judiciary has sufficient technical knowledge and understanding. To that end, I concur with the recommendation of Susan Hennessey of the

[279] 18 U.S.C. §2518(4)

Brookings Institution that the Federal Judicial Center develop a manual to educate judges who are charged with evaluating warrant applications for lawful hacking. Furthermore, the use of court-appointed neutral technical experts should be accepted as the norm.[280]

2. Long-Term Strategies

With respect to long-term strategies, the government must put some of its resources toward a public relations and education campaign to regain the public's trust and to garner more cooperation and information-sharing support from private industry. Data-mining firms like Recorded Future and Babel Streets may serve as open-source intelligence to supplement and assist. Apple might be persuaded to once again cooperate with responding to subpoenas for plain text data stored on iCloud. Increasing transparency in the Vulnerabilities Equities Process and including delegates from the technology industry in the process will restore good faith and strengthen cooperation.

With respect to winning public support, the solution to the going dark problem cannot be framed as a choice between collective security and individual privacy. It is important to emphasize that the public needs not abandon any hope for privacy. The NSA's past mass–data-collection practices notwithstanding, the solution proposed is one that is narrowly tailored to target individual suspects for surveillance and protects the civil liberties of all.

Surveillance of a targeted few bad individuals planning to carry out bad acts also protects the privacy of the rest of society. It is not fear-mongering to present a context in which our other liberties, such as freedom of travel, may be compromised in the wake of a terrorist attack. It is reality. One only has to refer to the state of emergency imposed by the French government in the wake of the Paris attacks to realize what other civil liberties French citizens are deprived of. More extreme examples would be failed states around the globe, such as Iraq and Syria, where their citizens' safety and basic human rights are violated every day, let alone civil liberties like individual privacy. It is this message that

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

the U.S. government must deliver to the public: Americans must think not only of what liberties are constricted, but what liberties are protected in adopting lawful hacking as the solution to the going dark problem.

Furthermore, what is often lost in this debate is the fact that the government is pursuing *lawful* and *targeted* surveillance as opposed to the mass–data-collection practices of the NSA. The two practices often get conflated with *lawful* surveillance bearing the blame of the public mistrust. Law enforcement and intelligence officials must highlight this point every time they discuss the going dark problem. They must also point out that just as it is unwise to build in vulnerabilities to communications infrastructure, it is just as unwise to build a communications infrastructure that is warrant-proof. As Benjamin Wittes writes on *Lawfare*, an argument for a surveillance-free Internet is an argument for the world's largest ungoverned space. Just as it was an overreaction on the part of government in passing the Patriot Act in the wake of 9/11, it is an overreaction on the part of industry to oppose *all* types of government surveillance in the wake of the Snowden leaks. I believe that over a period of time, with consistent delivery of these issues, the American public will be more apt to support lawful hacking as a solution. More importantly, the public will do so understanding the risks and benefits and not out of fear.

B. CONCLUSION

For nearly a decade, law enforcement agencies, most vocally represented by the FBI, have been sounding the alarm about losing one of their most effective investigative tools due to the proliferation of end-to-end encryption. It is only getting worse. Since Apple first announced in late 2014 its intention of designing its devices and operating systems with default encryption with only the users holding the key, other device manufacturers and Internet-based communications platforms have followed suit. Meanwhile, crime and the threat of terrorism have not receded and the acrimony in the encryption debate has not abated.

The tension between collective security versus individual liberty is not new, but it is not often as polarizing as is presented in the going dark problem. Perhaps this is due to

the libertarian strain that was a part of the development of the Internet from the beginning. Perhaps this is also due to the growth of mistrust of the government from the Nixon era and further exacerbated by the Snowden leaks of NSA bulk–data-collection activities. Whatever the history, the time has come for a reasoned and middle-ground approach to solving the going dark problem. As Professor Lawrence Lessig wrote, the choice is not between "regulation" and "no regulation" of cyberspace but between the regulators. If the government does nothing, it is the computer code that regulates our interactions in cyberspace simply because code is able to implement values, enable freedoms, or disable them. Code also protects privacy or promotes monitoring. But code is written or designed by people—the coders—who are not representatives of ordinary people and who have not been sworn to uphold our constitutional values.[281] Thus, taking no legislative action and leaving the coders to implement their own values and dictate their own ideas of collective security is not an option that comports with representative democratic principles. Therefore, the status quo is not acceptable. Congress must act.

This thesis endeavors to advance the debate over encryption toward concrete policy proposals to resolve the going dark problem. To this end, it has made recommendations for a way in which law enforcement may lawfully exploit vulnerabilities that already exist in any device, software, platform or network to conduct electronic surveillance in a limited number of cases. Government's lawful hacking will be conducted under strict judicial oversight and with clear minimization requirements. This solution is imperfect, but it is firmly planted in the narrow middle ground between frequently and diametrically opposing interests and viewpoints. As a middle-ground solution, it should make everyone happy that there is a formal policy addressing ubiquitous encryption that has been long overdue. At the same time, it will make no one happy that the policy is not perfectly aligned with their interests and ethics. In the end, the starting point must be the recognition and acceptance that there are tradeoffs to be made by both sides of the going dark debate.

---

[281] Lawrence Lessig, "Code Is Law," *The Industry Standard* 18 (1999).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner "Keys Under Doormats." *Communications of the ACM* 5, no. 10 (2015): 24-26.

Ahonen, Tomi. "Smartphone Wars: Q3 Scorecard—All Market Shares, Top 10 Brands, OS Platforms, Installed Base." Communities Dominate Brands, October 30, 2015. http://communities-dominate.blogs.com/brands/2015/10/smartphone-wars-q3-scorecard-all-market-shares-top-10-brands-os-platforms-installed-base.html.

Bankston, Kevin. "It's Time to End the Debate on Encryption Backdoors." *Just Security*, July 7, 2015.

Begley, Sharon. "Foiling the Clipper Chip." *Newsweek*, June 12, 1994. http://www.newsweek.com/foiling-clipper-chip-188912.

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, 19 (2014). http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip.

Benner, Katie, and Eric Lichtblau. "U.S. Says It Has Unlocked iPhone Without Apple." *New York Times*. Accessed March 29, 2016. http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.

Berkman Center for Internet and Society and Harvard University. "Don't Panic Making Progress on Going Dark Debate." February 1, 2016. https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Bernstein, D. J. "Summary of Case Status, Bernstein v. U.S. DOJ." Accessed November 19, 2016. http://cr.yp.to/export/status.html.

Bilge, Leyla, and Tudor Dumitras. "Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World." *Proc. 2012 ACM Conf. on Computer & Comm. Security*, 2012.

Bobbitt, Philip. *Terror and Consent, The Wars for the Twenty First Century*. New York: Anchor, 2008.

Caldwell, Leslie. “Additional Considerations Regarding the Proposed Amendments to the Federal Rules of Criminal Procedure.” U.S. Department of Justice, November 28, 2016. https://www.justice.gov/opa/blog/additional-considerations-regarding-proposed-amendments-federal-rules-criminal-procedure.

———. “Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation.” U.S. Department of Justice, November 21, 2016. https://www.justice.gov/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation.

Cardozo, Nate, and Andrew Crocker. “Deep Dive into Crypto ‘Exceptional Access’ Mandates: Effective or Constitutional—Pick One.” Electronic Frontier Foundation, August 13, 2015. https://www.eff.org/deeplinks/2015/08/deep-dive-crypto-exceptional-access-mandates-effective-or-constitutional-pick-one.

Clarke, Richard, Michael Morell, Jeffrey Stone, Cass Sunstein, and Peter Swire. “Liberty and Security in a Changing World, Report and Recommendations from the President’s Review Group on Intelligence and Communications Technologies.” December 12, 2013. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Cloud, Morgan. “A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment.” *Ohio State Journal of Criminal Law* 3 (2005): 33-73.

Comey, James. “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” Washington, DC: Brookings Institution, 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, February 16, 2016. https://www.apple.com/customer-letter/.

Crocker, Andrew, and Jamie Williams. “Deep Dive: Why Forcing Apple to Write and Sign Code Violates the First Amendment.” March 3, 2016, Electronic Frontier Foundation. Accessed February 3, 2017. https://www.eff.org/deeplinks/2016/03/deep-dive-why-forcing-apple-write-and-sign-code-violates-first-amendment.

Diffie, Whitfield, and Martin Hellman. “New Directions in Cryptography.” *IEEE Transactions on Information Theory,* IT-22, November 6, 1976.

Donahue, Laura K. “Section 702 and the Collection of International Telephone and Internet Content.” *Harvard Law Journal and Public Policy* 38 (2015): 117, 199.

Electronic Frontier Foundation. “The Playpen Cases: Mass Hacking by U.S. Law Enforcement.” August 15, 2016. https://www.eff.org/cases/playpen-cases-mass-hacking-us-law-enforcement.

English, Charles M. “Compelled Speech and the First Amendment: Neutral Fact or Government Opinion?” Legal Backgrounder, Washington Legal Foundation 27, no. 1 (January 13, 2012). http://www.wlf.org/upload/legalstudies/legalbackgrounder/1-13-12English_LegalBackgrounder.pdf.

Federal Rules of Criminal Procedure. “Rule 41. Search and Seizure.” Accessed December 13, 2016. https://www.federalrulesofcriminalprocedure.org/title-viii/rule-41-search-and-seizure/.

Freitas, Nathan. “6 Ways Law Enforcement Can Track Terrorists in an Encrypted World.” *MIT Technology Review,* November 24, 2015. https://www.technologyreview.com/s/543896/6-ways-law-enforcement-can-track-terrorists-in-an-encrypted-world/.

Gilbert, David. “Apple Removes *New York Times* from App Store to Keep Chinese Government Happy.” VICE News, January 5, 2017. https://news.vice.com/story/apple-removes-new-york-times-from-app-store-to-keep-chinese-government-happy.

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

Greenwald, Glen. “FISA Court Oversight: A Look Inside a Secret and Empty Process.” *Guardian,* June 18, 2013. https://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy.

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

———. “Vulnerabilities Equities Reform That Makes Everyone (And No One) Happy.” Lawfare, July 8, 2016. https://www.lawfareblog.com/vulnerabilities-equities-reform-makes-everyone-and-no-one-happy.

Homeland Security Committee. “Final Report of the Task Force On Combating Terrorist And Foreign Fighter Travel.” September 2015. https://homeland.house.gov/wp-content/uploads/2015/09/TaskForceFinalReport.pdf.

Hosenball, Mark. “FBI Paid under $1 Million to Unlock San Bernardino iPhone: Sources.” Reuters, May 4, 2016. http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032.

Inspire. “How to Communicate with Us.” 1434, no. 11 (Spring 2013). https://azelin.files.wordpress.com/2013/05/inspire-magazine-issue-11.pdf

Jaffer, Jamil, and Daniel Rosenthal. “Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge.” *Catholic University Journal of Law and Technology* 24, no. 2 (May 24, 2016): 289.

Jagadish, H. V. “Encryption, Cybersecurity, Privacy, Terrorism.” Homeland Security News Wire. Accessed March 4, 2016. http://www.homelandsecuritynewswire.com/dr20160224-passwords-privacy-and-protection-can-apple-meet-fbi-s-demand-without-creating-a-backdoor.

Jaycox, Mark. “EFF Opposes McCaul-Warner Encryption Commission.” Electronic Frontier Foundation, March 16, 2016. https://www.eff.org/deeplinks/2016/03/eff-opposes-mccaul-warner-encryption-commission.

Kahn, David. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner, 1996.

Kayyali, Dia. “What You Need to Know About the FISA Court and How It Needs to Change.” Electronic Frontier Foundation, August 15, 2014. https://www.eff.org/deeplinks/2014/08/what-you-need-know-about-fisa-court-and-how-it-needs-change.

Kehl, Danielle. “Encryption 101.” Slate, February 24, 2015. http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html.

Kehl, Danielle, Andi Wilson, and Kevin Bankston. “Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s.” New America. https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf.

Kerr, Orin S. “Applying the Fourth Amendment to the Internet: A General Approach.” *Stanford Law* Review 62, no. 4 (2009): 1005–50.

Lapowsky, Issie. “After Paris, Encryption Will Be a Key Issue in the 2016 Race.” *Wired*, November 17, 2015.

Lessig, Lawrence. “Code Is Law.” The Industry Standard 18 (1999).

———. *Code: And Other Laws of Cyberspace*. New York: Basic Books, 1999.

Liptak, Adam. “Supreme Court Says Phones Can’t Be Searched Without a Warrant.” *New York Times*, June 25, 2014. http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html.

Liu, Edward C. “Reauthorization of the FISA Amendment Act.” CRS Report No. 42725, Washington, DC: Congressional Research Service, 2013.

Lynch, Jennifer. “New FBI Documents Provide Details on Government’s Surveillance Spyware.” Electronic Frontier Foundation, April 29, 2011. https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government.

Manhattan District Attorney’s Office. “Smartphone Encryption and Public Safety.” November 2015. http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety, 9.

———. “Smartphone Encryption and Public Safety.” November 2016, p. 32. https://assets.documentcloud.org/documents/3222483/White-Paper-2-0.pdf#page=3.

McAdams III, James G. "Foreign Intelligence Surveillance Act (FISA): An Overview.” https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf.

MEMRI Cyber & Jihad Lab. “Al-Fajr Technical Committee Releases Android App for Secure Communication, Announces New Website.” June 11, 2014. https: http://cjlab.memri.org

Nakashima, Ellen. “FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone.” *Washington Post*, April 12, 2016. https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

Nakashima, Ellen, and Andrea Peterson. “Obama Faces Growing Momentum to Support Widespread Encryption.” *Washington Post*, September 16, 2015

National Security Council. “Draft Options Paper on Strategic Approaches to Encryption.” 2015. Accessed May 13, 2016. https://assets.documentcloud.org/documents/2426450/read-the-nsc-draft-options-paper-on-strategic.pdf.

Office of Public Affairs. “Colorado and Illinois Men Sentenced to Prison for Engaging in Child Exploitation Enterprise.” U.S. Department of Justice, October 18, 2016. https://www.justice.gov/opa/pr/colorado-and-illinois-men-sentenced-prison-engaging-child-exploitation-enterprise.

Perlroth, Nicole. “Security Experts Oppose Government Access to Encrypted Communication.” *New York Times*, July 7, 2015.

Perlroth, Nicole, and David E. Sanger. “Obama Won’t Seek Access to Encrypted User Data.” *New York Times*, October 10, 2015. http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html.

Pham, Sherisse. “Apple Yanks *New York Times* Apps in China.” CNNMoney, January 5, 2017. http://money.cnn.com/2017/01/05/technology/apple-nyt-china-app-store-remove/index.html.

President's Council of Advisors on Science and Technology. *Big Data and Privacy: A Technological Perspective.* Washington, DC: White House, 2014.

Recorded Future. “How Al Quaeda Uses Encryption Post Snowden, Part 1.” May 8, 2014. https: www.recordedfuture.org.

———. “How Al-Qaeda Uses Encryption Post-Snowden, Part 2.” August 1, 2014. https:www.recordedfuture.org.

Riley, Michael. “NSA Said to Have Used Heartbleed Bug, Exposing Consumers.” Bloomberg.com, April 11, 2014. https://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.

Risen, James, and Eric Lichtblau. “Bush Lets U.S. Spy on Callers Without Courts.” *New York Times*, December 16, 2005. http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

Rotenberg, Marc, and Alan Butler. “Symposium: In Riley v. California, a Unanimous Supreme Court Sets out Fourth Amendment for Digital Age.” SCOTUSblog, June 26, 2014. http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/.

Rowan, Beth. “Post 9/11 Changes by the U.S. Government.” InfoPlease. Accessed September 30, 2015. http://www.infoplease.com/us/history/911-anniversary-government-changes.html.

Sanger, David E. “Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say.” *New York Times*, April 12, 2014. https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html.

Savage, Charlie. “Surveillance Court Rules that NSA Can Resume Bulk Data Collection.” *New York Times*, June 30, 2015. https://www.nytimes.com/2015/07/01/us/politics/fisa-surveillance-court-rules-nsa-can--resume-bulk-data-collection.html.

Schneier, Bruce. “Back Doors Won’t Solve Comey’s Going Dark Problem.” Lawfare, 2015. https://www.schneier.com/blog/archives/2015/07/back_doors_wont.html.

———. *Data and Goliath.* New York: W.W. Norton, 2015.

———. “Disclosing vs. Hoarding Vulnerabilities.” Schneier on Security, May 22, 2014. https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html.

———. “The NSA Is Hoarding Vulnerabilities.” Schneier on Security, August 26, 2016. https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html.

Schwartz, Ari, and Rob Knake. “Government’s Role in Vulnerabilities Disclosure: Creating a Permanent and Accountable Vulnerability Equity Process” The Cyber Security Project, Belfer Center for Science and Security Affairs, Harvard Kennedy School, 2016, 4. http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf.

Shatchman, Noah. “Exclusive: Google, CIA Invest in ‘Future’ of Web Monitoring.” *Wired*, July 28, 2010

Simcox, Robin. “Surveillance After Snowden.” *Henry Jackson Society*, 2015, 62.

Singh Guliani, Neema. “4 Problems With Creating a ‘Commission on Encryption,’” Washington Markup, March 9, 2016. https://www.aclu.org/blog/washington-markup/4-problems-creating-commission-encryption.

Solove, Daniel. “Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference.” *Fordham Law Review* 74, no. 2 (2005): 747, 775.

Sulmasy, Glen, and John Yoo. “Katz and the War on Terrorism.” *UC Davis Law Review* 41, no. 3 (2008): 1227. http://lawreview.law.ucdavis.edu/issues/41/3/intl-crime-terrorism/41-3_Sulmasy-Yoo.pdf.

Sydell, Laura. “In Apple Security Case, Obama Calls To Strike A Balance.” NPR.org. Accessed March 14, 2016. http://www.npr.org/2016/03/12/470194268/in-apple-security-case-obama-calls-to-strike-a-balance.

Thompson II, Richard R. “Digital Searches and Seizures: Overview of Rule 41 of the Rules of Criminal Procedures.” CRS Report No. R44547. Washington, DC: Congressional Research Service, September 8, 2016). https://www.hsdl.org/?view&did=795598.

Timberg, Craig. “Apple Will No Longer Unlock Most iPhones, iPads for Police, Even With Search Warrants.” *Washington Post*, September 14, 2014.

———. “Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police.” *Washington Post*, September 18, 2014.

Tyson, Jeff. “How Encryption Works.” AllData N.S., August 15, 2016. http://alldatans.com/how-encryption-works/.

———. “How Encryption Works.” HowStuffWorks, April 6, 2001. http://computer.howstuffworks.com/encryption.htm.

Williams, Katie Bo. “FBI Shares Apple Vulnerability through Controversial Review.” The Hill, April 26, 2016. http://thehill.com/policy/cybersecurity/277845-fbi-used-controversial-wh-review-to-tell-apple-about-older-security-hole.

Wingfield, Nick, and Katie Benner. “Apple Is Rolling Up Backers in iPhone Privacy Fight Against F.B.I.” *New York Times*. Accessed March 6, 2016. http://www.nytimes.com/2016/03/04/technology/apple-support-court-briefs-fbi.html.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California