Catholic University Journal of Law and Technology

Volume 24 | Issue 2 Article 3

2016

Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge

Jamil N. Jaffer
George Mason University Law School

Daniel J. Rosenthal
Kroll

DECRYPTING OUR SECURITY: A BIPARTISAN ARGUMENT FOR A RATIONAL SOLUTION TO THE ENCRYPTION CHALLENGE

Jamil N. Jaffer & Daniel J. Rosenthal*

INTRODUCTION

Recent terrorist attacks in Garland, Texas,[1] Paris, France,[2] and more recently in Brussels, Belgium,[3] and San Bernardino, California,[4] have vividly demonstrated the increasing threat the United States faces at the hands of international terrorism. In the aftermath of the September 11, 2001 attacks, the U.S. gov-

* Jamil N. Jaffer is an Adjunct Professor of Law and Director of the Homeland and National Security Law Program at the George Mason University School of Law. Mr. Jaffer previously served in a variety of national security positions in the legislative and executive branches, including in the Bush Administration as Associate Counsel to the President and as Counsel to the Assistant Attorney General for National Security at the Department of Justice and also as a Senior Counsel to the House Intelligence Committee. Daniel J. Rosenthal is an Associate Managing Director with Kroll, a global leader in investigations, risk mitigation, compliance, security, and incident response solutions. He also serves as an Adjunct Professor at the University of Maryland's Honors College, where he teaches an award-winning course on national security dilemmas. Mr. Rosenthal previously served in a variety of national security positions in the Obama Administration, including as Director for Counterterrorism with the National Security Council, as Senior Counsel to the Assistant Attorney General for National Security at the Department of Justice, and as a Senior Associate General Counsel for the Director of National Intelligence. The authors would like to thank Wendy Everette and Alexis Wilhelmi of George Mason University Law School for their excellent research assistance.

1 Manny Fernandez, Richard Pérez-Peña & Fernanda Santos, *Gunman in Texas Shooting Was F.B.I. Suspect in Jihad Inquiry*, N. Y. TIMES (May 4, 2015), http://nyti.ms/1ABVyYf.

2 Anthony Faiola & Souad Mekhennet, *Paris Attacks Were Carried Out By Three Groups Tied To Islamic State, Official Says*, WASH. POST (Nov. 15, 2015) http://wapo.st/1HJk4zJ.

3 Karen Yourish et al., *Brussels is Latest Target in Islamic State's Assault on West,* N.Y. TIMES (Mar. 25, 2016), http://nyti.ms/1VrAz7y.

4 Adam Nagourney, Ian Lovett & Richard Pérez-Peña, *San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead*, N. Y. TIMES (Dec. 2, 2015), http://nyti.ms/1Tw5gWG.

ernment has taken major steps, over the course of years, to bolster its ability to detect and thwart attacks on the homeland.[5] These tools—in particular the collection of content of overseas communications pursuant to the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008[6]—have proven critical to the government's ability to protect the homeland from terrorist threats.[7] Alarmingly, as a direct result of the devastating disclosures of classified information—including the details of this program's operation—by Edward Snowden in June 2013,[8] terrorists have gained significant insight into the ability of the United States to gain access to their electronic communications, and therefore, have taken steps to change their communications methods and tactics, including through the widespread adoption of encryption technologies to hide their communications,[9] in an attempt to evade law enforcement and plot future

---

5 *See, e.g.*, Memorandum from Jack L. Goldsmith, III, Office of Legal Counsel to the Attorney General, Review of the Legality of the STELLAR WIND Program 7 (May 6, 2004) [hereinafter STELLAR WIND Memorandum], http://1.usa.gov/1LaJzfb (noting that in response to the September 11 attacks and to counter the ongoing threat posed by al Qaeda, in early October 2011, "the President directed the Secretary of Defense to use the capabilities of the Department of Defense, in particular the National Security Agency ("NSA"), to undertake a program of electronic surveillance designed to [] counter[] the threat of further al Qaeda attacks within the United States."); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

6 *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438 (2008) (codified at 50 U.S.C. § 1801 (2012)) (providing clear statutory authority under the supervision of the Federal courts for the United States to gain access, in the United States, to the global communications of foreign intelligence targets—including terrorists—located overseas).

7 *See* Letter from James R. Clapper, Director of Nat'l Intelligence & Eric H. Holder, Jr., Attorney General, to John Boehner, Speaker, Harry Reid, Majority Leader, Nancy Pelosi, Democratic Leader, Mitch McConnell, Republican Leader 2 (Feb. 8, 2012), http://1.usa.gov/1nsGiME ("Intelligence collection under Title VII has produced and continues to produce significant intelligence that is vital to protect the nation against international terrorism and other threats.").

8 Timothy B. Lee, *Here's Everything We Know About PRISM To Date*, WASH. POST (June 12, 2013), http://wapo.st/1QCGvZE; Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://wapo.st/1LcAw6p. Note that these articles include both information that the government may not have acknowledged as well as information that may or may not be accurate. *See infra* text accompanying note 52.

9 Joe Palazzolo, *FBI Stymied by Islamic State's Use of Encryption, Director Says*, WALL ST. J. (Nov. 18, 2015, 1:53 PM), http://on.wsj.com/1O3fc9Z; Benjamin Wittes, *What Role Did Encryption Play in Paris?*, LAWFARE (Nov. 16, 2015, 7:40 AM), http://bit.ly/1R1oyQn; David E. Sanger & Nicole Perlroth, *Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks*, N.Y. TIMES (Nov. 16, 2015), http://nyti.ms/1MSkUpP; Shane Harris, *This is ISIS's New Favorite App for Secret Messages*, DAILY BEAST (Nov. 16, 2015, 8:00 PM), http://thebea.st/1SVu3mI.

attacks without any—or at most a greatly diminished—risk of detection.[10]

As a result of these tactical changes by terrorists, law enforcement has argued that its ability to identify and thwart future attacks to the homeland has been significantly diminished. Indeed, FBI Director James Comey recently characterized this widespread adoption by terrorists of encryption as a "grave" and "growing" threat to the country's national security.[11] Investigators now believe that the perpetrators of the attacks in Paris may have used encryption as a means of evading detection by law enforcement.[12] It is quite possible that the perpetrators of other recent attacks, such as Garland, Texas and San Bernardino, California, did so as well.[13]

---

[10] For the purposes of this paper, the term encryption means the conversion of plaintext into ciphertext using an algorithm to render the data unreadable without the proper cipher and key to decrypt it. *See* NAT'L INST. OF STANDARDS AND TECH., NISTIR 7298 REV. 2, GLOSSARY OF KEY INFORMATION SECURITY TERMS 69 (Richard Kissel ed. 2013), http://1.usa.gov/1Q7m0We ("Encryption Algorithm: Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key."). Strong encryption generally refers to encryption with particularly long key lengths. *See* NORMAN D. JORSTARD & LANDGRAVE T. SMITH, INST. FOR DEF. ANALYSES, 20NCDROM, CRYPTOGRAPHIC ALGORITHM METRICS 15 (1997), http://1.usa.gov/1Tnlepb.

> Street and Walker have recently suggested a three graduation scale for indicating the strength of cryptography based on key length: 'Weak Cryptography,' applications with secret keys of 40 bits (DES, RC2, RC4), and for public key 512 bits or less; 'Good Cryptography,' secret key of 56 bits (typically DES), public key 512 to 1024 bits; and, 'Strong Cryptography,' secret key lengths in excess of 56 bits and public keys that are 1024 bits and larger.

Id. (internal footnotes and citations omitted); *see also* MANHATTAN DIST. ATT'YS OFF., REPORT ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 2 (2015) [hereinafter MANHATTAN D.A.'S REPORT], http://bit.ly/1WYUIVq.

> Encryption involves converting readable data (sometimes referred to as "plaintext") into scrambled, unreadable data (sometimes referred to as "ciphertext") using an algorithm that renders the data unreadable by a human or computer without the proper cipher and key to decrypt it. Data transmitted between phones, computers, and other digital devices can be encrypted [] while in transit between those devices and [] on the devices themselves.

Id.

[11] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary* 114th Cong. 10 (2015) [hereinafter *Going Dark Hearing*] (joint statement of Sally Quillian Yates, Deputy Att'y Gen., Department of Justice, and James B. Comey, Director, Federal Bureau of Investigation), http://1.usa.gov/1Xd65VE ("Mr. Chairman, the Department of Justice believes that the challenges posed by the Going Dark problem are grave, growing, and extremely complex").

[12] Ben Wittes, *Thoughts on Encryption and Going Dark: Part I*, LAWFARE (July 9, 2015, 10:29 AM) [hereinafter Wittes, *Going Dark: Part I*], http://bit.ly/1LN77qr; Paul Tassi, *How ISIS Terrorists May Have Used PlayStation 4 To Discuss And Plan Attacks*, FORBES (Nov. 14, 2015, 6:17 PM), http://onforb.es/21TMT5M *but see* Bruce Schneier, *Paris Terrorists Used Double ROT-13 Encryption*, SCHNEIER ON SEC. (Nov. 18, 2015, 3:35 PM), http://bit.ly/1YhriPA.

[13] Danny Yadron, *Does Encryption Really Help ISIS? Here's What You Need to Know*,

Even as terrorists take action to secure themselves against American surveillance, the overall quantity of terrorist attacks worldwide—including those directed at the West—are on the rise,[14] and it is nearly inevitable that we will continue to be victimized by smaller-scale attacks such as those we have recently experienced. While the groups plotting terrorist attacks worldwide today—a cast of characters that includes ISIS, al Qaeda, and their affiliates—face very real difficulties in pulling off a mass casualty attack on the homeland on a scale akin to the attacks on September 11, 2001, there is little doubt that they have the ongoing intent, and are constantly plotting, to do so.[15] And, without continuous, aggressive action to take the fight to these terrorist groups overseas and continued vigilance at home supported by strong law enforcement and intelligence efforts, there is a serious chance that they will succeed in pulling off another major attack in the coming years. In our view—born of significant national security experience on both sides of the political spectrum and in various branches of the federal government[16]— the growing trend towards

---

WALL ST. J.: DIGITS (Dec. 4, 2015, 11:37 AM), http://on.wsj.com/1Svrfiq.

[14] *See generally* U.S. DEP'T OF STATE, COUNTRY REPORTS ON TERRORISM 2014, at 8, 11, 16-17, 25 (2015), http://1.usa.gov/1IV1G3y.

[15] The recent attacks in Paris and San Bernardino were perpetrated at the direction of, or at least were inspired by, the Islamic State of Iraq and Syria ("ISIS"). *See* Rukmini Callimachi, *ISIS Claims Responsibility, Calling Paris Attacks 'First of the Storm'*, N. Y. TIMES (Nov. 14, 2015), http://nyti.ms/1Nxm5eZ; *see also* Missy Ryan et al., *Both San Bernardino Attackers Pledged Allegiance To The Islamic State, Officials Say,* WASH. POST (Dec. 8, 2015) http://wapo.st/24MSA4H. These attacks vividly demonstrate the increasing risk of terrorist attacks on the homeland that we face at the hands of international terrorists. ISIS, and other violent terrorist groups including the Khorasan Group, Al-Qa'ida in the Arabian Peninsula ("AQAP"), and the various affiliates and offshoots of these organizations, remain committed to raising a generation of killers who predicate their violence on a distorted view of Islam to spread their totalitarian ideology, impose their oppressive way of life around the world, and cause as many deaths as they can to non-adherents. And while ISIS initially spent significant time and capital on its localized ambitions to establish an operational government in Iraq and Syria, they are now, alarmingly, focusing much more of their attention on planning or inspiring attacks in the West, including the United States homeland. *See* Graeme Wood, *What ISIS Really Wants*, THE ATLANTIC (March 2015), http://theatln.tc/1N4APrk; *see also* Paul D. Shinkman, *The Evolving Extremist Threat,* U.S. NEWS (Dec. 7, 2015, 6:17 PM), http://bit.ly/1UOaOyj.

[16] It is worth noting that a number of presidential candidates—in both parties—have decisively raised this issue also, calling for rational solutions. *See, e.g.*, *Hillary Clinton Lays Out Comprehensive Plan To Bolster Homeland Security,* THE BRIEFING (Dec. 15, 2015), http://hrc.io/1W4mbR5.

> Now, encryption of mobile devices and communications does present a particularly tough problem with important implications for security and civil liberties. Law enforcement and counterterrorism professionals warn that impenetrable encryption may make it harder for them to investigate plots and prevent future attacks. On the other hand, there are very legitimate worries about privacy, network security, and creating new vulnerabilities that bad actors can exploit. I know there's no magic fix to this di-

default-on, ubiquitous strong encryption, while providing critically important privacy and security benefits, also means the United States is more likely to face challenges in preventing the next major terrorist attack in the West.

As such, we must act now to address the encryption challenge. Doing so is not only the responsible thing to do to protect our nation, but it maximizes the chances that we can continue to protect the legitimate—and critically important—privacy and security benefits that ubiquitous strong encryption provides to freedom activists, consumers, technologists, and most importantly, the average citizen, every day. Because security means very little without privacy, and vice versa, the current debate—which is polarized between those who claim that government access to encrypted communications is either impossible or will destroy both security and privacy on the Internet and those who claim that a lack of access to such data will mean that the government "goes dark," essentially flying blind while trying to stop active threats—is vastly unhelpful and highly unlikely to reach a stable result. Privacy groups, having already won a bruising battle on similar questions in the 1990s and having called significant portions of the technology industry to arms in the aftermath of the Snowden disclosures,[17] are feeling their oats as they see the Justice Department and FBI unable to gain ground in their efforts to take more aggressive steps to regain lawful access to encrypted communications.[18] Likewise, law enforcement and intelligence agencies, licking their wounds after having lost these battles, are increasingly turning to authorized disclosures, or leaks, regarding use of encryption by terrorist groups in active plots and threats in the hopes

---

> lemma that will satisfy all these concerns. But we can't just throw up our hands. The tech community and the government have to stop seeing each other as adversaries and start working together to keep us safe from terrorists. And even as we make sure law enforcement officials get the tools they need to prevent attacks, it's essential that we also make sure jihadists don't get the tools they need to carry out attacks.

Id.; *see also* Patrick Kulp, *Jeb Bush Says He Would Compel Tech Companies to Hand Over Encrypted Data If President*, MASHABLE (Jan. 15, 2016), http://on.mash.to/1puDqAy (noting that former Gov. Jeb Bush suggested that he might require companies to cooperate with government requests for information and argued that "[t]here needs to be complete dialogue with large technology companies…[t]hey understand there's a national security risk."); Jenna McLaughlin, *Jeb Bush Comes Out Against Encryption*, THE INTERCEPT (Aug. 19, 2015, 3:40 PM), http://bit.ly/1nsi0Cu (statement of Florida Governor Jeb Bush).

> If you create encryption, it makes it harder for the American government to do its job — while protecting civil liberties — to make sure that evildoers aren't in our midst…We need to find a new arrangement with Silicon Valley in this regard because I think this is a very dangerous kind of situation.

Id.

[17] David Sirota, *Has America Changed Since Edward Snowden's Disclosures?,* TRUTHDIG (June 14, 2015), http://bit.ly/1puDv7B.

[18] *See* Nicole Perlroth & David E. Sanger*, Obama Won't Seek Access to Encrypted User Data*, N.Y. TIMES (Oct. 10, 2015) [hereinafter Perlroth & Sanger, *Obama Won't Seek Access*], http://nyti.ms/1G6YAvL.

that these efforts will vividly demonstrate the problem and garner support for more aggressive measures before the next major attack.[19]

While today the pendulum has decisively swung in the direction of those that oppose law enforcement and intelligence access to encrypted data, in our view, this is almost certainly an unsustainable balance. The reason is simple: we know, without question, that terrorist groups are using encryption to protect themselves from government surveillance;[20] and we also know that these groups continue to plot significant, mass casualty attacks against the United States and our allies.[21] When combined with the fact that multiple states have recently failed or are failing in the Middle East[22] and ISIS continues to expand its territorial control in its effort to build a terrorist superstate—a state of play that provides opportunities for terrorist groups to coalesce, plan, and execute attacks[23]—there is a significant possibility that a major terrorist attack, planned using encrypted communications and likely more deadly than the recent horrific attacks in Paris and San Bernardino, will take place in the United States or Europe.

When that day comes, unfortunately for those of us who believe that a rational balance between privacy and security is possible, any opportunity to design a security solution that appropriately accounts for what are very real, important, and legitimate privacy considerations will have been lost. As it was in the immediate aftermath following September 11, 2001,[24] the political climate will likely provide little opportunity for any meaningful dialogue between the technology sector, advocacy groups, and the government to work together to find a sensible solution. Rather, in the wake of the next catastrophic attack on the homeland, the law enforcement and national security communities will likely be offered significant authority to address the encryption challenge, and at that point, in the scramble to quickly shore up the nation's defenses against terrorists, the government will have little to no incentive to work with the most

---

19 *Id.*

20 Kim Zetter, *Security Manual Reveals the OPSEC Advice ISIS Gives Recruits*, WIRED (Nov. 19, 2015, 4:45 PM), http://bit.ly/21XeBeG.

21 DAVID INSERRA, HERITAGE FOUND., ISSUE BRIEF NO. 4416, 69TH ISLAMIST TERRORIST PLOT: ONGOING SPIKE IN TERRORISM SHOULD FORCE CONGRESS TO FINALLY CONFRONT THE TERRORISM THREAT 1 (2015), http://bit.ly/1R1piVB.

22 Lee Ferran & Rym Momtaz, *ISIS Trail of Terror*, ABC NEWS (Feb. 23, 2015), http://abcn.ws/1rouSL7.

23 *Id.* (attributing ISIS's success to the group's use of the combination of "military expertise and unimaginable brutality" combined with taunting social media accounts and weak government forces).

24 *See* Jeffrey Rosen, *Total Information Awareness*, N.Y. TIMES (Dec. 15, 2002), http://nyti.ms/1AA5cu1 (discussing the Bush administration's Total Information Awareness Program, an attempt to implement information-sharing to prevent terrorism in response to the September 11 Attacks, and the opposition of privacy advocates to the program).

important communities of interest on the outside. Indeed, it is likely the government already has, or will quickly generate, draft legislation to address these issues that does not fully account for legitimate privacy and cybersecurity concerns.

Therefore, if the technology sector and advocacy groups are to realistically have a seat at the table, the time for action is now. While such a suggestion may seem counterintuitive given the fact that the current political climate—at least prior to the Paris and San Bernardino attacks—was strongly favorable to the views of the technology community and advocacy groups, given the threat, the possibility of a significant attack, and the likelihood that the use of encryption facilitates the success of such an attack, as well as the political climate that such a situation is virtually certain to engender, relying on the current climate is a mistake. Indeed, if we fail to take smart steps now, it is highly likely that action taken in the wake of future attacks will gut the hard-won gains made by privacy groups since the 1990s.

The reason why is simple. Defending "warrant-proof" encryption[25] on the merits is already a challenge today, and will likely become impossible in the aftermath of an attack. For all of the deeply-felt, strongly-held, and longstanding skepticism of the government action, particularly when justified under the banner of national security, the American people have always acknowledged that the government plays an essential role in protecting physical security and that liberties must, at some level, give way to the government's legitimate activities, particularly in the realm of national security.[26] It is for this very reason

---

[25] *See Going Dark Hearing*, *supra* note 11.

> [I]ncreasingly, we're finding that even when we have the authority to search certain types of digital communications, we can't get the information we need because the encryption has been designed so that the information is only available to the user and the providers are unable to comply with the court order or warrant….Crucial information becomes, in effect, 'warrant proof.'….[W]e can't get access to information that is stored on someone's smartphone, like a child pornographer's photographs or a gang member's saved text messages…And we also can no longer effectuate wiretap orders to intercept certain communications as they happen, like ISIL members plotting to carry out an attack in the U.S., or a kidnapper communicating with a coconspirator… ISIL currently communicates on Twitter, sending communications to thousands of would-be followers right here in our country. When someone responds and the conversations begin, they are then directed to encrypted platforms for further communication. And even with a court order, we can't see those communications. This is a serious threat and our inability to access these communications, with valid court orders, is a real national security and public safety problem.

Id.; *see also* Andrea Peterson, *The Government and Privacy Advocates Can't Agree On What 'Strong' Encryption Even Means*, WASH. POST (Oct. 7, 2015), http://wapo.st/1RPfRvA (statement of Kiran S. Raj, Senior Counsel to the Deputy Attorney General at the Department of Justice) ("Warrant-proof encryption, as distinct from strong encryption, is where you design a system in a manner where only the end user has access to the information.").

[26] Carroll Doherty, *Balancing Act: National Security and Civil Liberties in Post-9/11*

that the first ten amendments, while at times seemingly absolute in their language, have always been understood to allow for reasonable action by the government.[27] And, indeed, in the case of the Fourth Amendment—the core protection against the type of government action that encryption is designed to limit—the very notion of reasonable government access is actually built into the text.[28] As was the case following the September 11th attacks, and as we are currently seeing in Europe, otherwise privacy-focused countries will often tilt strongly towards security in the aftermath of a major terrorist incident.[29] And though we may hope that this won't be the case this time and that cooler heads will prevail, such hope is ephemeral at best and likely makes for bad policy decisions now.

Yet, despite the urgency of this problem, and despite the increased awareness of the threat posed to the homeland from terrorism, the United States' decision-making architecture is paralyzed; voices within the government,[30] the technology sector,[31] and the advocacy community[32] argue that any effort to

---

Era, PEW RES. CTR. (June 7, 2013), http://pewrsr.ch/1M3zHyM (stating that generally since 9/11, Americans have valued national security over their civil liberties).

27 *See, e.g.*, Emp't Div., Dep't of Hum. Res. of Oregon v. Smith, 494 U.S. 872, 888-90 (1990) (upholding as constitutional a prohibition on the use of peyote because the prohibition was neutrally applicable and served a compelling government interest even though it conflicts with the free practice of religion); Goldman v. Weinberger, 475 U.S. 503, 507 (1986) (upholding a Navy uniform regulation that conflicted with a religious requirement).

28 The Fourth Amendment provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* searches and seizures shall not be violated." U.S. CONST., amend. IV. (emphasis added); *see also* City of Los Angeles v. Patel, 135 S. Ct. 2443, 2451-52 (2015) (citing Arizona v. Gant, 556 U.S. 332, 338 (2009)) (explaining that the Constitution only bars unreasonable searches). The Supreme Court has recognized as reasonable searches conducted by the government in a number of scenarios in which a warrant is impractical, including when necessary for public safety and in exigent circumstances. *See* New York v. Quarles, 467 U.S. 649, 655-59 (1984) (creating a public safety exception in instances in which fulfilling the Miranda requirements would impede time-sensitive efforts to advance public safety); Chambers v. Maroney, 399 U.S. 42, 48-49 (1970) (establishing a car search exception to the warrant requirement); Michigan v. Fisher, 558 U.S. 45, 46 (2009) (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006)) (holding that police may enter a home without a warrant under the emergency aid exception); United States v. Santana, 427 U.S. 38, 42–43 (1976) (holding that police may enter a home without a warrant in hot pursuit of a suspect).

29 Russell B. Wilson, A New Balance: National Security and Privacy in a Post 9-11 World 3-4 (2014) (unpublished Honors Thesis, Colby College), http://bit.ly/1YzWau7.

30 Perlroth & Sanger, *Obama Won't Seek Access*, *supra* note 18.

31 Eric Newcomer, *Apple CEO Defends Encryption, Opposes Government Back Door*, BLOOMBERG BUS. (Oct. 20, 2015, 3:08 AM), http://bloom.bg/1nsij0b; Orin Kerr, *Apple's Dangerous Game*, WASH. POST (Sept. 19, 2014) [hereinafter Kerr, *Apple's Dangerous Game*], http://wapo.st/1pbMvOS.

32 Joseph Lorenzo Hall, *Strong Encryption Has a Posse*, CTR. FOR DEMOCRACY & TECH. (May 20, 2015), http://bit.ly/1R3P4i6.

undermine terrorists' ability to use encryption to communicate necessarily undermines the availability of encryption for beneficent purposes.[33] And the national security establishment clings desperately to its metaphor that the government is "going dark" despite its failure to date (by virtue of inability or unwillingness) to demonstrate clearly to the public that its capabilities overall have dropped off dramatically.[34]

As a result of the overheated rhetoric on both sides, the nation now finds itself in the throes of a dangerous stalemate. The privacy and technology community believes it is winning, and therefore feels no need to negotiate; to the contrary it continues to press the government to be even less active than it already is; and the national security community, continuously raising the alarm and not content to continue to wait, also understands that events may significantly change the state of play in their favor.[35] The outcome of this stalemate is plain as day: The government is being squeezed into inaction on the legislative and regulatory fronts, and is instead settling for modest efforts to initiate some voluntary cooperative work with an industry that is likely to have little, if any, substantive impact on the very real issues at stake.[36]

---

[33] Andrea Peterson & Ellen Nakashima, *Obama Administration Explored Ways To Bypass Smartphone Encryption,* WASH. POST (Sept. 24, 2015), http://wapo.st/1R2rjTv; Bruce Schneier, *Why We Encrypt*, SCHNEIER ON SEC. (June 23, 2015, 6:02 AM), http://bit.ly/1GlWG54.

[34] *See Going Dark Hearing*, *supra* note 11, at 5.

[35] *See, e.g.*, Ellen Nakashima & Andrea Peterson, *Obama Faces Growing Momentum to Support Widespread Encryption*, Wash. Post (Sept. 16, 2015), http://wapo.st/20sbB8r; Kim Zetter, *After Paris Attacks, Here's What the CIA Director Gets Wrong About Encryption*, WIRED (Nov. 16, 2015, 5:50 PM), http://bit.ly/1LaK5d6.

> Robert S. Litt, general counsel in the Office of the Director of National Intelligence, predicted as much in an email sent to colleagues three months ago. In that missive obtained by the Washington Post, Litt argued that although "the legislative environment [for passing a law that forces decryption and backdoors] is very hostile today, it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."

Id.

[36] Perlroth & Sanger, *Obama Won't Seek Access, supra* note 18.

> The Obama administration has backed down in its bitter dispute with Silicon Valley over the encryption of data on iPhones and other digital devices…While the administration said it would continue to try to persuade companies like Apple and Google to assist in criminal and national security investigations, it determined that the government should not force them to breach the security of their products…"As the president has said, the United States will work to ensure that malicious actors can be held to account, without weakening our commitment to strong encryption," said Mark Stroh, a spokesman for the National Security Council. "As part of those efforts, we are actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. However, the administration is not seeking legislation at this time."

Id.

The two authors of this article both served as senior counterterrorism and national security officials for Presidents from different parties: Jamil Jaffer served in the White House and Justice Department during the George W. Bush Administration, and Daniel (DJ) Rosenthal served in the White House and Justice Department during the Barack Obama Administration. Each served Presidents from different political parties; there are issues relating to national security on which they disagree, including with regard to ways in which former President Bush sought to protect the nation from terrorism, and ways in which President Obama is currently seeking to do so. However, both authors firmly believe in the rule of law, and our nation's sacred and enduring commitment to privacy and civil liberties even as we seek to address the relentless threats posed by terrorism. They have co-authored this article because both vigorously agree on the critical need for our government, privacy, and technology communities to come together and act now to address the challenges posed by the current threat environment and shifting tactics, so that these authors are simultaneously not blind to the next terrorist attack on our homeland, and so that we can ensure that we preserve the huge privacy and economic benefits that we gain from ubiquitous strong encryption.

It is important to note that this policy essay, due primarily to space constraints, does not purport to be a full recounting of all the legal or policy issues or debates at play in the encryption discussions. Rather, the essay seeks to highlight a few areas where there are particular challenges, where the law continues evolve, and where some reasonable options have been put on the table. Part I sets out some of the key content surveillance laws put in place after the terrorist attacks of September 11, 2001, describes the current threat the nation faces, and the challenges that default-on, ubiquitous strong encryption poses for national security. Part II identifies the basic terms of the encryption debate. Part III describes a few aspects of the legal structures that have to be dealt with in the context of encryption. Part IV discusses a few key proposals that might usefully be considered as we seek to move forward on addressing these issues and Part V briefly summarizes our position on these matters—namely that security and privacy are best served by finding common ground on the encryption matter now, in the relative calm, rather than waiting to act in the aftermath of an attack when security will already have been sacrificed and privacy will pay a significant long term cost.

PART I: KEY SURVEILLANCE AUTHORITIES, THE THREAT, AND THE CHALLENGES POSED BY ENCRYPTION

Following the September 11, 2001 terrorist attacks in the United States, na-

tional security professionals worked hard to identify and fill gaps that existed in their ability to gather critical national intelligence about terrorist actors operating overseas.[37] They quickly recognized that the Foreign Intelligence Surveillance Act ("FISA"), [38] which Congress enacted in 1978 to govern electronic surveillance conducted within the United States for foreign intelligence purposes, was unintentionally impeding national security investigations by requiring a court order before the government could gain access to communications that are not entitled to constitutional protections—communications of non-U.S. persons overseas.[39] Because Congress was focused, in enacting FISA, on protecting the rights of Americans in the United States, and primarily with respect to their domestic communications, it defined "electronic surveillance" in a particular manner by reference to the location of the parties to the communication, the location in which the acquisition occurred, and the physical transmission layer of the communication.[40] In doing so, the drafters of FISA intended to include within its coverage key types of communications taking place within the

---

[37] *See Statement Before the House Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence Washington, D.C.* (2012) (statement of Eric Belez-Villar, Assistant Director, Directorate of Intelligence, Federal Bureau of Investigations); *The Post-9/11 Era (September 2001 – present): Legislative Materials*, LAWFARE (last visited Feb. 18, 2016), http://bit.ly/1U8L8vD.

[38] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§1801-1863 (2012)).

[39] *See* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1331-33 (2004); *see also* Robert S. Litt, General Counsel, Office of the Director of National Intelligence, Privacy, Technology & National Security: Remarks at the Brookings Institution (July 18, 2013), http://bit.ly/1pbMJ8R ("As a result [of technological advances], Congress's original intention was frustrated; we were increasingly forced to go to the FISA Court to get individual warrants to conduct electronic surveillance of foreigners overseas for foreign intelligence purposes.").

[40] *See* Foreign Intelligence Surveillance Act of 1978 § 101(f); Robert S. Litt, General Counsel, Office of the Director of National Intelligence, Privacy, Technology & National Security: Remarks at the Brookings Institution (July 18, 2013), http://bit.ly/1pbMJ8R.

> When FISA was first passed in 1978, Congress did not intend it to regulate the targeting of foreigners outside of the United States for foreign intelligence purposes. This kind of surveillance was generally carved out of coverage under FISA by the way Congress defined 'electronic surveillance.' Most international communications in 1978 took place via satellite, so Congress excluded international radio communications from the definition of electronic surveillance covered by FISA, even when the radio waves were intercepted in the United States, unless the target of the collection was a U.S. person in the United States. Over time, that technology-based differentiation fell apart. By the early twenty-first century, most international communications travelled over fiber optic cables and thus were no longer "radio communications" outside of FISA's reach.

Id.; *see also* Philip M. Bridwell & Jamil N. Jaffer, *Updating the Counterterrorism Toolkit: A Brief Sampling of Post-9/11 Surveillance Laws and Authorities*, ADMIN. & REG. L. NEWS, Spring 2011, at 19-20.

United States or acquired through certain methods inside the United States.[41] At the same time, Congress intentionally excluded a significant portion of the international communications traffic to and from the United States—traffic that took place over satellites when FISA was enacted—or what FISA referred to as "radio."[42] With the passage of time, however, this technology-based distinction evaporated, as fiber optic cables increasingly transmitted international communications, or "wire" in FISA parlance, and domestic calls made via cellphones, were increasing transmitted by wireless or "radio."[43]

As a result of these changes in technology, communications that were never governed by FISA, and that Congress never intended to regulate under FISA, were subjected to its stringent rules, which required that the government seek a court order—under the same standard it must meet for U.S. persons—in its efforts to track terrorists overseas.[44] This requirement hindered the government's ability to gain access to terrorist communications, often in fast-moving critical national security investigations.[45]

To address this gap, the government initiated a program to target the communications content of non-U.S. terrorists overseas without having to seek a court order.[46] While there exists residual criticism about the means by which

---

41 *See id.* at 18-20; Stephanie Cooper Blum, *What Really Is At Stake With The FISA Amendments Act Of 2008 And Ideas For Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 278 (2009).

42 *See* Bridwell & Jaffer, *supra* note 40, at 18-20; *see also* H. REP. NO. 95-1283, pt.1, at 27 (1978) ("The committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances."); S. REP. NO. 95-604, pt.1, at 34 (1977) ("The reason for excepting from the definition of electronic surveillance the acquisition of international radio transmissions, including international wire communications when acquired by intercepting radio transmissions, is to exempt from the procedures of this bill the signals intelligence activities of the National Security Agency.").

43 Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 148 (2015).

44 *See* Kate Poorbaugh, *Security Protocol: A Procedural Analysis Of The Foreign Intelligence Surveillance Courts*, 2015 U. ILL. L. REV. 1363, 1373 (2015).

45 *Id.* at 1373-77; L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits*, 66 VAND. L. REV. 1343, 1394-96 (2013); William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2157-58 (2002).

46 STELLAR WIND Memorandum, *supra* note 5, at 7-8.

> [T]he President directed the Secretary of Defense to use the capabilities of the Department of Defense, in particular the National Security Agency (NSA), to undertake a program of electronic surveillance designed to…countering the threat of further al Qaeda attacks within the United States….The electronic surveillance activities that the President authorized under STELLAR WIND…[included the] interception of the content of certain communications … the President noted that he had considered magnitude and probability of deaths and destruction that could result from further terrorist

the government first built this program in the immediate aftermath of September 11, 2001,[47] Congress eventually expressly authorized the program in statute and subjected it to Article III judicial supervision, through passage of the Protect America Act in 2007 and subsequently the FISA Amendments Act in 2008.[48] This program–codified in Section 702 of FISA–has proven to be critical in the government's counterterrorism efforts.[49] Senior intelligence community officials have repeatedly noted that collection under Section 702 is one of the most valuable counterterrorism tools available to the national security community, and Executive branch officials and members of Congress from both political parties have identified numerous instances in which collection under Section 702 has enabled the government to thwart what could have been significant terrorist attacks in the U.S. and abroad before they were executed.[50]

> attacks; the need to detect and prevent such attacks, particularly through effective electronic surveillance…Upon consideration of these factors, the President determined that…this emergency constituted…supported conducting the described surveillance without resort to judicial warrants.

Id.; Stephen J. Schulhofer, *Spies, Secrets, And Security: The New Law of Intelligence: The Foreign Intelligence Surveillance Act: The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV 531, 539 (2006).

47 *See, e.g.*, Jeffrey S. Brand, *Eavesdropping on Our Founding Fathers: How a Return to the Republic's Core Democratic Values Can Help Us Resolve the Surveillance Crisis*, 6 HARV. NAT'L SEC. J. 1, 42 (2015) (referring to a FISA court judge's resignation in response to the "illegal" Stellar Wind program); David Husband, *Who Decides? Drawing the Lines in the National Security Realm*, 8 FED. CTS. L. REV. 245, 297 (2015) (arguing that the development of the surveillance programs was secretive and "the American public was not brought on board.").

48 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§1801-1863 (2000)); *see also* Poorbaugh, *supra* note 44, at 1375.

49 *See* Press Release, James R. Clapper, Director of Nat'l Intelligence, DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013), http://1.usa.gov/1nsGiME ("Section 702 has proven vital to keeping the nation and our allies safe. It continues to be one of our most important tools for the protection of the nation's security."); *see also* Letter from James R. Clapper & Eric H. Holder, Jr. to John Boehner, Harry Reid, Nancy Pelosi, & Mitch McConnell*, supra* note 7, at 3.

> Section 702 is vital in keeping the nation safe. It provides information about the plans and identities of terrorists, allowing us to glimpse inside terrorist organizations and obtain information about how those groups function and receive support. In addition, it lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States. Failure to reauthorize section 702 would result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities.

Id.

50 *See Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs: Hearing Before the S. Comm. on the Judiciary,* 113th Cong. 12 (2013) (statement of Sean M. Joyce, Deputy Director, Federal

During the summer of 2013, news outlets released a number of stories based on documents they had received from former NSA contractor Edward Snowden that ostensibly detailed highly classified activities of the intelligence community, including the alleged means by which it obtains communications of terrorists overseas under Section 702 of FISA.[51] While many of the stories had inaccuracies, material declassified by the government has since made it clear that significant aspects of the government's collection architecture were revealed in the course of these leaks.[52]

Almost immediately following the leaks, terrorists began changing their tactics to evade detection.[53] Among other things, according to FBI Director Comey, terrorists began using computer and mobile messaging applications that enabled them to encrypt their communications, which poses significant challenges to the ability of the law enforcement and national security communities to discover and disrupt terrorist plotting.[54] Exacerbating the problem, after Snowden's leak, leading technology companies have taken voluntary steps that make the government's efforts to track terrorists more difficult.[55]

Bureau of Investigation), http://1.usa.gov/222GIMO.

[51] *See* Barton Gellman & Todd Lindeman, *Inner Workings of a Top-Secret Spy Program*, WASH. POST (June 29, 2013), http://wapo.st/1QCHVmR (outlining how the PRISM program works); Gellman & Poitras, *supra* note 8.

[52] *See* Press Release, Office of Dir. of Nat'l Intelligence, Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013) (on file with author).

[53] Barbara Starr*, Terrorists Try Changes After Snowden Leaks, Official Says*, CNN (June 25, 2013, 6:27 PM), http://cnn.it/1M3uh71 ("We can confirm we are seeing indications that several terrorist groups are in fact attempting to change their communications behaviors based specifically on what they are reading about our surveillance programs in the media.").

[54] *Oversight of the Federal Bureau of Investigation*, *Statement Before the S. Comm. on the Judiciary*, 114th Cong. (2015) [hereinafter *FBI Oversight Statement*] (statement of James B. Comey, Director, Federal Bureau of Investigation).

> While some of the contacts between groups like ISIL and potential recruits occur in publicly accessible social networking sites, others take place via encrypted private messaging platforms. This real and growing gap, which the FBI refers to as 'Going Dark,' is an area of continuing focus for the FBI; we believe it must be addressed, since the resulting risks are grave both in both traditional criminal matters as well as in national security matters.

Id.; Geoff Dyer & Barney Jopson, *Encryption Harms Terror Probes, Says FBI*, FIN. TIMES (Dec. 9, 2015), http://on.ft.com/1UOc0Sd.

[55] Cyrus Farivar, *Apple Expands Data Encryption Under iOS 8, Making Handover to Cops Moot*, ARS TECHNICA (Sept. 18, 2014, 12:57 AM), http://bit.ly/XL1tx9; Brad Smith, *Protecting Customer Data from Government Snooping*, MICROSOFT BLOG (Dec. 4, 2013), http://bit.ly/1QyKRzC; *Safer Email – Transparency Report*, GOOGLE, http://bit.ly/1Ypxy7L (last visited Feb. 21, 2016); Pierluigi Paganini, *IT Giants Google and Apple Enable Encryption by Default,* SEC. AFFAIRS (Sept. 20, 2014), http://bit.ly/21TOtor; Leon Spencer, *Android L Will Offer Default Encryption Just Like iOS 8*, ZDNET (Sept. 19, 2014),

Many companies have publicly disclaimed any voluntary cooperation with government, legitimately fearing the public fallout, particularly in Europe, if they are viewed as being too close to the federal government.[56] These companies have also taken affirmative steps to protect their users' data through the implementation of strong encryption for data in transit, as well as data at rest.[57]

Apple,[58] for example, implemented default-on, strong encryption for data at rest on its devices.[59] Indeed, prior to the release of iOS 8, Apple was able to use "a proprietary method to extract data from the device" to access and provide to the government content information stored on Apple devices in response to court authorized warrants.[60] In September 2014, Apple announced

---

http://zd.net/1D8MN8s; Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption*, *Blocking Police,* WASH. POST (Sept. 18, 2014), http://wapo.st/1nsj6hG.

[56] Matt Apuzzo, David E. Sanger, & Michael S. Schmidt, *Apple and Other Tech Companies Tangle with U.S. Over Data Access*, N.Y. TIMES (Sept. 7, 2015), http://nyti.ms/21XfMuy.

[57] *Id;* Sam Thielman, *US and European Officials Reignite 'Back Door' Encryption Debate After Paris*, THE GUARDIAN (Nov. 18, 2015, 7:00 AM), http://bit.ly/1QH6BXY. For the purposes of this paper, "data at rest" means information stored on devices while "data in transit" or "data in motion" means information as it is being transferred from one source to another. *See* Simon Liu & Rick Kuhn, *Data Loss Prevention,* IT PRO, March/April 2010, at 10, 11-12 ("[D]ata at rest, meaning it resides in files systems, distributed desktops and large centralized data stores, databases, or other storage centers" and "data in motion, meaning it moves through the network to the outside world via email, instant messaging, peer-to-peer (P2P), FTP, or other communication mechanisms."); *see also* MANHATTAN D.A.'S REPORT, *supra* note 10, at 2.

> "Data at rest" is information that is stored on devices after the data-creating event has occurred. Data at rest could include, for example, a text message that has been received by a smartphone and has not been deleted from the device…."Data in transit" refers to information in the very moment that it is being transferred from one source to another, for example, information communicated in a phone conversation is data in transit while it is being transferred.

Id.; *see also* James Comey, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Remarks Before the Brookings Institution. (Oct. 16, 2014) [hereinafter Comey, Brookings Institution Remarks], http://1.usa.gov/1ClnQNc.

> The first [challenge] concerns real-time court-ordered interception of what we call 'data in motion,' such as phone calls, e-mail, and live chat sessions" and "court-ordered access to data stored on our devices, such as e-mail, text messages, photos, and videos—or what we call 'data at rest.'…[B]oth real-time communication and stored data are increasingly encrypted.

Id.; While at rest, data may be stored, among other things, on a local device, on a network store, or at a service provider "in the cloud." *See* Liu & Kuhn, *supra* note 57, at 12-13.

[58] This note does not seek to address the arguments and relative merits of the government's efforts, in California and New York, to seek to compel Apple's assistance in obtaining access to data contained on encrypted iPhones. These matters are rapidly evolving and are being covered extensively elsewhere.

[59] MANHATTAN D.A.'S REPORT, *supra* note 10, at 1-3.

[60] *Id.* at 4.

> With respect to the iPhone 4s and later models of iPhones and other Apple devices

that iOS 8 would automatically encrypt all data at rest on its device when locked such that information could only be accessed provided that the appropriate passcode was entered.[61] With this change, and unlike prior versions of iOS, Apple is now unable to access data stored on its devices using this operating system, even if law enforcement provides Apple with a court-authorized warrant.[62] Later versions of iOS have included the same capability enabled by

---

> running iOS versions through iOS 7…law enforcement requires the assistance of Apple to obtain the devices' contents safely. The prosecutor or investigator obtains a search warrant and an order (often referred to as an "unlock order") instructing Apple to assist with extracting data from the device. The prosecutor or investigator then sends Apple a copy of the warrant, the unlock order, the device, and a blank external hard drive. Apple uses a proprietary method to extract data from the device, and sends a copy of the data to law enforcement on the external hard drive.

Id.; Kerr, *Apple's Dangerous Game*, *supra* note 31.

> Under the old operating system, Apple could execute a lawful warrant and give law enforcement the data on the phone. Under the new operating system, that warrant is a nullity. It's just a nice piece of paper with a judge's signature. Because Apple demands a warrant to decrypt a phone when it is capable of doing so, the only time Apple's inability to do that makes a difference is when the government has a valid warrant.

Id.

[61] *Privacy – Our Approach to Privacy*, APPLE, http://apple.co/1RPgqWe (last visited Feb. 27, 2016).

> We build privacy into everything we make…. We've been protecting your data for over a decade with SSL and TLS in Safari, FileVault on Mac, and encryption that's built into iOS. We also refuse to add a 'backdoor' into any of our products because that undermines the protections we've built in. And we can't unlock your device for anyone because you hold the key — your unique password. We're committed to using powerful encryption because you should know the data on your device and the information you share with others is protected.

Id.; Joe Miller, *Google and Apple To Introduce Default Encryption*, BBC NEWS (Sept. 19, 2014), http://bbc.in/1sav1lF; Nate Raymond, *Apple Tells U.S. Judge 'Impossible' To Unlock New Iphones*, REUTERS (Oct. 20, 2015), http://reut.rs/1LN5dpX.

> In court papers, Apple said that for the 90 percent of its devices running iOS 8 or higher, granting the Justice Department's request 'would be impossible to perform' after it strengthened encryption methods. Those devices include a feature that prevents anyone without the device's passcode from accessing its data, including Apple itself. The feature was adopted in 2014 amid heightened privacy concerns following leaks by former National Security Agency contractor Edward Snowden about NSA surveillance programs.

Id.

[62] *See* MANHATTAN D.A.'S REPORT, *supra* note 10, at 4.

> For Apple devices running iOS 8, Apple can no longer comply with unlock orders. iOS 8 prevents Apple from accessing data on the device unless Apple has the user's passcode. But, Apple does not keep users' passcodes. Thus, it is no longer possible for Apple to extract data as it did for devices running prior operating systems.

Id.

default.[63]

As a result, as of October 2015, the data at rest on approximately 91% of iPhones worldwide—a percentage that is incrementally increasing—is inaccessible to law enforcement, even with a court-authorized warrant.[64] In the U.S. alone—which as of mid-2015 had an iPhone installed user base of approximately 94 million, a number that is increasing—more than 85 million devices from Apple alone are likely off limits to law enforcement.[65] This doesn't even account for the estimated 463 million iOS devices in use worldwide.[66]

Google made a similar announcement with respect to data at rest on Android devices running Lollipop 5.0 or higher and, while implementation of default-on encryption has been sporadic amongst Google partners due to performance issues on Lollipop 5.0 devices, Google's own Nexus phones with Lollipop 5.0 have default-on encryption enabled.[67] With over one third of Android devices

---

[63] *See* Miller, *supra* note 61*; see also Privacy – Our Approach to Privacy*, *supra* note 61.

[64] *See* MANHATTAN D.A.'S REPORT, *supra* note 10, at 4. ("According to Apple, as of October 19, 2015, approximately 61% of all Apple devices currently in use run iOS 9, and approximately 30% use iOS 8. Only nine percent use an earlier iOS version."); *see also App Store – Support – Apple Developer,* APPLE, http://apple.co/1QH7a4a (last visited Jan. 11, 2016) (noting that as of January 11, 2016, 94% of Apple devices worldwide use iOS 8 or higher).

[65] *See* Press Release, Consumer Intelligence Research Partners, Significant iPhone 6, 6 Plus Penetration in U.S. (May 15, 2015) (on file with author); *see also* Don Resinger, *iPhones In Use in the US Rise to 94M, New Study Suggests*, CNET (May 15, 2015, 10:18 AM), http://cnet.co/1RxlMCW.

[66] *See* Tomi T. Ahonen, *Smartphone Wars: Q3 Scorecard - All Market Shares, Top 10 Brands, OS Platforms, Installed Base*, COMMUNITIES DOMINATE BRANDS BLOG (Oct. 30, 2015, 4:36 AM), http://bit.ly/1TFI2Rq.

[67] Kevin Tofel, *Google Now Requires Full Device Encryption On New Android 6.0 Devices*, ZDNET (Oct. 19, 2015, 7:48 PM), http://zd.net/1U0j4M8; *see also* MANHATTAN D.A.'S REPORT, *supra* note 10, at 5.

> For Android devices running operating systems Lollipop 5.0 and above, however, Google plans to use default full-disk encryption, like that being used by Apple, that will make it impossible for Google to comply with search warrants and orders instructing them to assist with device data extraction. Full-disk encryption has not yet been implemented as a default on all Android devices running Lollipop 5.0 and later systems, but has been implemented on certain Nexus (Google-controlled) devices.

Id.; Lucian Constatin, *Google Requires Full-Disk Encryption and Secure Boot for Some Android 6.0 Devices*, COMPUTERWORLD (Oct. 20, 2015, 7:04 AM), http://bit.ly/1M549Hn.

> With the release of Android 6.0, the Android Compatibility Definition Document (CDD)…now lists full-disk encryption as a requirement instead of a recommendation. If a device does not declare itself as a low-memory device—with about 512MB of RAM—and supports a secure lock screen, it must also support full-disk encryption of both the application data and shared storage partitions, the document says. Furthermore, if the device has an Advanced Encryption Standard (AES) cryptographic operation performance above 50MB/s, the full-disk encryption feature must be enabled by default during the initial set-up.

using Lollipop 5.0 or higher,[68] and an installed base of 1.8 billion devices worldwide,[69] Google's implementation of this approach likewise significantly increases the challenge for law enforcement agencies seeking to use court-authorized warrants to obtain content data from smartphones.[70] Because people are continuing to increase their use of mobile devices, as opposed to traditional desktop or laptop computers, to communicate,[71] this trend poses major challenges to law enforcement's ability to conduct its investigations.

PART II: TERMS OF THE DEBATE

Given these trends, the change in tactics described earlier, and the fact that public key encryption is virtually unbreakable,[72] the increased determination and ability of international terrorists to carry out attacks is a cause for signifi-

---

Id.; Timberg, *supra* note 55.

68 *See Dashboards – Android Developers,* GOOGLE (Feb. 1, 2016), http://bit.ly/18oBxX9 (noting distribution rates of Lollipop 5.0 at 17%, Lollipop 5.1 at 17.1%, and Marshmallow 6.0 at 1.2%).

69 *See* Ahonen, *supra* note 66; *cf*. Press Release, Gartner, Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments On Pace to Grow 7.6 Percent in 2014 (Jan. 7, 2014), http://gtnr.it/1eEJ08k ("Android holds the largest number of installed-base devices, with 1.9 billion in use in 2014, compared with 682 million iOS/Mac OS installed-base devices.").

70 *See* MANHATTAN D.A.'S REPORT, *supra* note 10, at 5.

71 MONICA ANDERSON, PEW RES. CTR., TECHNOLOGY DEVICE OWNERSHIP: 2015, at 3 (2015), http://pewrsr.ch/1WarhLx (noting that smartphone ownership has increased 33 percentage points to 68% since 2011, while desktop and laptop ownership has stayed at ~72% since 2004).

72 *Commerce, Justice, Science, and Related Agencies Appropriations for 2016: Hearing Before the S. Comm. on Commerce, Justice, and Science of the H.R. Comm. on Appropriations*, 115th Cong. 21 (2015) (statement of James B. Comey, Director, Federal Bureau of Investigation), http://1.usa.gov/1parFyR ("We have a huge problem for law enforcement…and in national security work. We have court process, where judges issue search warrants or interception orders, and we are unable to execute on those orders because the device is locked or the communications are encrypted."); Wittes, *Going Dark: Part I*, *supra* note 12 (quoting James B. Comey, Director Federal Bureau of Investigation) ("[I]f we intercept data in motion between two encrypted devices or across an encrypted mobile messaging app and it's strongly encrypted, we can't break it."); *see also* Paul Rosenzweig, *Encryption, Biometrics, and the Status Quo Ante*, LAWFARE (July 6, 2015, 10:29 AM) [hereinafter Rosenzweig, *Encryption, Biometrics*], http://bit.ly/1R1rxYY.

> But there is a technological flip-side to the conversation that pro-encryption advocates too often disregard – the reality that properly implemented encryption is, for all practical purposes, uncrackable.")The advent of public key encryption has, effectively changed the public policy dynamic – never before in human history have we seen a means of communication that was theoretically immune from government interception and access…[P]ublic key encryption is, in theory, beyond mathematical analysis. It is impenetrable. That's a real change.

Id.

cant concern. Secretary of Homeland Security Jeh Johnson has recently noted that "today the global terrorist threat is more decentralized, more complex, and in many respects harder to detect."[73] Government officials argue that widespread adoption of encryption by terrorists worldwide could cripple the government's ability to detect and disrupt terrorists, including those who intend to carry out attacks inside the United States.[74] FBI Director James Comey has characterized the increasing challenge in detecting terrorist plots as a result of encryption—which he and other government officials refer to as "going dark"—as posing a "grave" and "growing" threat to national security.[75] Comey has also noted that while the FBI is tirelessly working to identify individuals who seek to join ISIS as well as "homegrown violent extremists who may aspire to attack the United States from within,"[76] terrorists' increasing use of encryption "poses real barriers" to its ability to gather critical information necessary to thwart the next attack.[77]

For example, Comey has said that 109 text messages between the Garland shooters and overseas terrorists remain inaccessible due to the use of encryption[78] and has testified that the use of encrypted communications is now standard "terrorist tradecraft."[79] In particular, Comey has warned of the potential threat to the homeland posed by homegrown extremists recruited by ISIS

---

[73] *Threats to the Homeland, Hearing Before the S. Comm. on Homeland Sec. & Gov't Affs.,* 114th Cong. (2015) (written statement of Jeh Johnson, Secretary, Department of Homeland Security), http://1.usa.gov/1R1rAUu.

[74] Alina Selyukh & Steve Henn, *After Paris Attack, Encrypted Communication Is Back In Spotlight*, NPR (Nov. 6, 2015, 5:29 PM), http://n.pr/1l0OSBr (quoting New York Police Commissioner Bill Bratton as saying that it is a very significant negative effect on our ability to detect and disrupt terrorist activity).

[75] *Threats to the Homeland, Hearing Before the S. Comm. on Homeland Sec. & Gov't Affs.,* 114th Cong. (2015) (statement of James B. Comey, Director, Federal Bureau of Investigation), http://1.usa.gov/1OXWQTe.

[76] *Id.*

[77] *Going Dark Hearing*, *supra* note 11, at 9-10.

[78] 161 Cong. Rec S8,664 (daily ed. Dec. 15, 2015) (statement of James B. Comey, Director, Federal Bureau of Investigation), http://1.usa.gov/22fvwZM; Pierre Thomas, *Feds Challenged by Encrypted Devices of San Bernardino Attackers*, ABC NEWS (Dec. 9, 2015, 6:04 PM), http://abcn.ws/1Ncu7wq ("'There's no doubt that use of encryption is part of terrorist tradecraft now,' Comey told the Senate Judiciary Committee. 'Increasingly, we are unable to see what they say, which gives them a tremendous advantage against us.'"); Melanie Hunter, *FBI Director: Terrorist in Texas Attack Sent 109 Encrypted Messages on Morning of Attack to Terrorist Overseas,* CNS NEWS (Dec. 9, 2015, 3:45 PM), http://bit.ly/1QH7IH2 ("'We have no idea what he said,' Comey said about one of the gunmen, 'because those messages were encrypted, and to this day, I can't tell you what he said with that terrorist 109 times the morning of that attack. That is a big problem. We have to grapple with it…'").

[79] *See* Thomas*, supra* note 78*; see also* Jonathan Alter, *Manhattan DA: Smartphone Encryption Foiled 120 Criminal Cases*, The DAILY BEAST (Dec. 28, 2015, 12:13 AM), http://thebea.st/1p3hs7o.

online who may be using encrypted means to communicate with ISIS recruiters and operatives overseas.[80] Comey argues that the FBI's "job is to find needles in a nationwide haystack, needles that are increasingly invisible to us because of end-to-end encryption" and that because ""we don't have the capability we need," this really represents "the 'going dark' problem in high definition."[81] Perhaps most importantly, as Ben Wittes, co-founder of the Lawfare Blog, points out, "[a]s a practical matter, that means there are people in the United States whom authorities reasonably believe to be in contact with ISIS for whom surveillance is lawful and appropriate but for whom useful signals interception is not technically feasible."[82]

The President himself has highlighted the distinct nature of the terrorism challenge and the need to balance priorities. Specifically, the President recently noted:

> If we get into a situation which the technologies do not allow us at all to track somebody we're confident is a terrorist…and despite knowing that information, despite having a phone number or a social-media address or email address, that we can't penetrate that, that's a problem.[83]

The problem is not limited to terrorism. Manhattan District Attorney Cyrus Vance recently suggested that "more than 120 Manhattan criminal cases have been harmed by the failure to execute search warrants on the latest smartphones."[84] Vance also notes that criminals incarcerated at New York's Rikers Island prison often counsel their colleagues outside of the prison to use current-era iPhones because of the at-rest encryption they employ.[85] Vance extends this argument to the national security and cyber realms, arguing that "[i]f the average criminal at Rikers knows it, the terrorist knows it, the sophis-

---

80 *See FBI Oversight Statement, supra* note 54; *see also* Steven Melendez, *FBI Renews Warnings on Terror and Encryption, with No Clear Solution in Sight*, FAST CO. (Dec. 14, 2015, 12:15 PM), http://bit.ly/1NVlYxT.

81 *See* Theodore Schleifer, *FBI Director: We Can't Yet Restrain ISIS On Social Media*, CNN (June 18, 2015, 3:19 PM) (quoting James Comey, Director, Federal Bureau of Investigations), http://cnn.it/21hSWM1.

82 Ben Wittes, *Jim Comey, ISIS, and "Going Dark,"* LAWFARE (July 1, 2015, 5:17 PM), http://bit.ly/1puEHYy.

83 Cody M. Poplin, *President Obama Comments on Back-doors in Encryption*, LAWFARE (Jan. 16, 2015, 5:50 PM), http://bit.ly/1nsk5P1 ("[The President] continued by not[ing] the difficult and sometime tenuous balance between security, liberty, and privacy, and stated that debate with civil libertarians and privacy groups had been "useful.").

84 *See* Alter, *supra* note 79; *see also* MANHATTAN D.A.'S REPORT, *supra* note 10, at 9 (noting that between mid-September 2014 and mid-October 2015, "the Manhattan District Attorney's Office was unable to execute approximately 111 search warrants for smartphones 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.").

85 *See* Alter, *supra* note 79.

ticated cyber-criminal knows it."[86] But Vance doesn't stop there—he further argues that "[i]t's only a matter of time before there's an incident where we say, 'Who gave [Apple CEO] Tim Cook the right to decide whether a parent can find a lost child?'"[87]

Many in the government—and former government officials on the outside—place a significant amount of the blame for the current challenges on American technology companies like Apple and Google that, as described above, have begun implementing not only strong encryption on their devices, but have done so in default-on mode, and, in the case of Apple, have done so in a manner that (unlike in prior versions which also provided for strong data encryption) ensures data are no longer accessible to any party other than the end user, including the manufacturer itself.[88] Indeed, many have argued that the real problem for the government stems less from the increasingly widespread availability of strong encryption itself and more from the shift by technology companies to make this capability available in "default-on" mode, which some have suggested—albeit without any actual testable data—could put 80-90% of data at rest in an encrypted and (ostensibly) warrant-proof state.[89] The more aggressive form of this argument from government officials—designed to undermine the widely employed rejoinder from technology companies, technologists, and privacy advocates that providing lawful access to encrypted content would require introducing unnecessary and damaging vulnerabilities to existing prod-

---

[86] *Id.*

[87] *Id.*

[88] *See, e.g.*, *Going Dark Hearing*, *supra* note 11, at 3.

> In recent months, however, we have on a new scale seen mainstream products and services designed in a way that gives users sole control over access to their data. As a result, law enforcement is sometimes unable to recover the content of electronic communications from the technology provider even in response to a court order or duly-authorized warrant issued by a Federal judge. For example, many communications services now encrypt certain communications by default, with the key necessary to decrypt the communications solely in the hands of the end user.

Id.

[89] *See* Rosenzweig, *Encryption, Biometrics*, *supra* note 72.

> The significance of the change that we are seeing is NOT in the development of public key encryption…Rather, the change is in the default rule – it is the difference between having encryption always 'off' as a default rule (such that people need to turn it on to be effective) and always 'on' (such that it works unless you turn it off). I have no data on how that change will affect government access to evidence of criminality, but my guess is that a default "on" rule will, once implemented and transitioned, put something on the order of 80-90% of data stored at rest in an encrypted state.

Id.; MANHATTAN D.A.'S REPORT, *supra* note 10, at 1 (discussing the Apple and Google announcements in 2014 regarding encryption in their product offerings, noting that "[t]he significance of the companies' change in practice was that this type of encryption would be the default setting on their new devices.").

ucts and services[90]—is that key companies have long possessed access to otherwise encrypted communications (in the case of Apple all the way until iOS 8 was released in September 2014) and many maintain such access as part of their business model (e.g., Google in the case of email content which it examines in order to push targeted ads to its customers) and yet none of these companies have suggested—until recently—that such provider access to such data introduces massive new vulnerabilities.[91]

As the debate over encryption has come to the fore once again, a wide range of civil society organization, advocacy groups, technology companies, trade associations, and security and policy experts have argued strongly against "any proposal that U.S. companies deliberately weaken the security of their products," urging the White House to "focus [instead] on developing policies that will promote rather than undermine the wide adoption of strong encryption technology."[92] These advocates correctly note that "[s]trong encryption is the cornerstone of the modern information economy's security" protecting consumers against fraud, companies against IP theft, and governments against foreign spies.[93]

The advocacy groups argue that the "mandatory insertion of any new vulnerabilities into encrypted devices and services" regardless of whether they are called front- or backdoors, "will make those products less secure against other attackers" and "would also seriously undermine our economic security…[because this] would further push many customers—be they domestic or international, individual or institutional—to turn away from those compro-

---

90 *See, e.g.*, HAROLD ABLESON ET AL., MASS. INST. OF TECH., MIT-CSAIL-TR-2015-026, KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS 2 (2015), http://bit.ly/1p3r16c.

> [B]uilding in exceptional access would substantially increase system complexity. Security researchers inside and outside government agree that complexity is the enemy of security — every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world….Features to permit law enforcement exceptional access across a wide range of Internet and mobile computing applications could be particularly problematic because their typical use would be surreptitious — making security testing difficult and less effective.

Id.

91 *See* LISA GEVELBER, GOOGLE, THE SHIFT TO CONSTANT CONNECTIVITY 3 (2013), http://bit.ly/1QCSeHH; NATE CARDOZO, KURT OPSAHL & RAINEY REITMAN, ELEC. FRONTIER FOUND., WHO HAS YOUR BACK? PROTECTING YOUR DATA FROM GOVERNMENT DATA REQUESTS 12 (2015), http://bit.ly/1puEPHl.

92 Letter from Civil Society Organizations, Companies and Trade Associations & Security and Policy Experts to President Barack Obama 1 (May 19, 2015), http://bit.ly/1IO8H77.

93 *Id.*

mised products and services."[94] The advocacy groups also question the benefits of requiring domestic providers to implement a lawful access program, pointing out that, rather than using government-accessible products from U.S. providers, bad actors will likely turn to foreign providers or use the wide variety of unregulated free and open source products available online to protect the privacy of their communications.[95] Finally, the groups note that any lawful access program required domestically could have the perverse effect of undermining human rights and democracy promotion efforts globally because other—less free—governments will be emboldened to seek similar access and the United States will be hard pressed to oppose such measures, having ceded the moral high ground and requiring such access domestically.[96] Such views are not limited to technology companies and advocates. The recent expert review panel convened by the President in the aftermath of the Snowden disclosures unanimously recommended the same thing: arguing that the U.S. Government should:

> (1) fully support[] and not undermin[e] efforts to create encryption standards; (2) mak[e] clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and (3) support[] efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.[97]

Moreover, former senior Bush Administration officials, including former Secretary of Homeland Security Michael Chertoff, DNI Michael McConnell, Deputy Secretary of Defense Bill Lynn, and Former CIA Director Gen. Michael V. Hayden—rarely shy on national security matters—have made similar arguments.[98]

---

[94] *Id*. at 1-2.

[95] *Id.*

[96] *Id.*

[97] *See* PRESIDENT'S REV. GRP. ON INTELLIGENCE & COMM'CNS TECH., LIBERTY AND SECURITY IN A CHANGING WORLD 22 (2013), http://1.usa.gov/1bK0q7x.

[98] *See, e.g.*, Michael McConnell, Michael Chertoff, and William Lynn, *Why the Fear Over Ubiquitous Data Encryption Is Overblown*, WASH. POST (July 28, 2015), http://wapo.st/1ShCPic.

> We recognize the importance our officials attach to being able to decrypt a coded communication under a warrant or similar legal authority. But the issue that has not been addressed is the competing priorities that support the companies' resistance to building in a back door or duplicated key for decryption. We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.

Id.; Jose Pagliery, *Ex-NSA Boss Says FBI Director Is Wrong On Encryption*, CNN (Jan. 13, 2016, 9:43 AM), http://cnnmon.ie/1nskmBp (statement of Gen. Hayden) ("I disagree with [FBI director] Jim Comey…I actually think end-to-end encryption is good for America…I know encryption represents a particular challenge for the FBI…[b]ut on balance, I actually think it creates greater security for the American nation than the alternative: a backdoor.");

Some have directly challenged the government's claim that it is "going dark." For example, a paper from Harvard's Berkman Center, co-authored by a number of prominent academics, practitioners, and technologists from varied backgrounds, takes issue with the notion that the government is going completely black—that is to say to entirely lose huge swaths of communications due to encryption.[99] In truth, the challenge the government faces is two-fold: first, the use of strong encryption by bad actors certainly creates new shadows and gaps where law enforcement will face more significant challenges if no forward progress is made on addressing lawful access to ciphertext, and second, when big providers start implementing strong encryption across the board and in a default-on mode, it simply makes potentially illicit uses that much harder to find as it allows bad actors to hide amongst the noise. This is not to suggest that ubiquitous strong encryption is not a net good, it is, but one must take into account that it does make the government's job that much harder. At the same time, however, the Berkman authors are also correct to point out that even as encryption may create new shadows and make the government's work harder at the margins, the velocity and nature of technological change and the integration of networked devices into entirely new areas of people's lives.[100] This of course includes the expansion of the vaunted Internet of Things ("IoT"), meaning that entirely new data flows soon will be opening up to law enforcement, thereby mitigating any loss from the expansion of encrypted communications.[101] The question of relative gains versus losses, of course, is an empirical one and a matter that neither the Berkman authors nor we propose to solve here. Rather, these are simply important issues to flag as we move forward and which highlight the fact that simple, formulaic statements like encryption is making the government "go dark" or seeking to address the challenge encryption poses to lawful access means "breaking the internet" or "sacrificing all security" are likely to muddy, rather than clarify the very real policy issues that require debate and discussion if we are to find a stable, sensible equilibrium.

At the same time, however, it is important to note that at least part of the Berkman authors' theory also faces some not unreasonable empirical challenges. For example, the Berkman authors argue that expanded access to data in the cloud and an expanded set of (presumably unencrypted) endpoints can make up for much of the data that might be lost as a result of key endpoints—like

---

see also Brad Reed, *Ex-NSA Chief Defends End-to-End Encryption, Says 'Backdoors' Will Make Us Less Secure*, BGR (Jan. 13, 2016, 12:57 PM), http://bit.ly/21hTjpI.

99 MATT OLSON, BRUCE SCHNEIER & JONATHAN ZITTRAIN, DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 2 (2016), http://bit.ly/1P0L1yW.

100 *Id.* at 3.

101 *Id.*

smartphones—employing default-on strong encryption.[102] The Manhattan District Attorney's office has challenged a key part of this claim head on, arguing that access to other sources, like iCloud or Google's data stores, does not fully compensate for a lack of access to encrypted smartphones.[103] Specifically, they argue that access to key types of data that would be found on a, iPhone, such as iMessage, SMS, certain cell tower related data, and third party app data simply aren't available on iCloud.[104]

On the other hand, the Manhattan District Attorney's report is also notable for what it highlights with respect to Google's cloud and server storage, which is that while many of the types of data available on an Android smartphone are not always going to be available in the Google Cloud, there is at least some opportunity for nearly all of the data to be available there.[105] The Manhattan District Attorney's report also notes that much of the data on a smartphone may not be available from the phone company.[106] Of course that's not surprising since one generally expects a telecommunications provider to principally provide data or content transport, not storage, and, to the extent it keeps any data, its likely to keep data relevant to the communications being transported, such as routing information and other such metadata.[107] While the Manhattan District Attorney's report argues, among other things, that "[e]ven under the best of circumstances, the cloud does not have all of the information that would be available on a personal device," that diversity and competition in the cloud storage space makes law enforcement's efforts more difficult, and that deleted data may not be recoverable from the cloud whereas it may be available on devices, the arguments simply aren't as robust as one might expect.[108] As such, while the Manhattan District Attorney's report takes a good shot at undermining the Berkman paper's argument at least as to iPhones, it really also serves to underline one of the Berkman paper's key findings which is—at least for providers who make money by accessing a significant measure of user information and content, like Google—encryption, particularly of data at rest, may be mitigated by ensuring lawful access to the same data that the company has access to for its own business purposes.[109]

Given these basic terms of the debate, it is also worth understanding the cur-

---

102 *Id.* at 9.

103 *See* MANHATTAN D.A.'S REPORT, *supra* note 10, at 6-8.

104 *Id.*

105 *Id.*

106 *Id.*

107 *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) (holding cell phone subscribers are aware that service providers use and collect their location data in order to connect their calls and for other billing and business records).

108 *See* MANHATTAN D.A.'S REPORT, *supra* note 10, at 8.

109 OLSON ET AL., *supra* note 99, at 10-12.

rent state of the law as it relates to some of these issues, particularly given that some of the recommendations currently under consideration or discussed in this paper would require changes in the law (and, after all, this is a law journal article).

PART III: LEGAL STRUCTURES

The examination of a few key legal structures relevant to the encryption debate focuses on a couple of the methods by which the government might conceivably access data stored on a smartphone or computer or in transit: (1) obtaining the access code to the device or the passphrase for the private key to the encryption being employed in the stored or transiting communication;[110] and (2) requiring the provider to build in a capability for the government, with technical assistance from the provider, to obtain lawful access to the content of communications.[111] Unfortunately for the government (and fortunately for those who support protection from government access), currently both of these avenues remain fairly challenging for the government.

With respect to simply obtaining access to the data from the end user by requiring them to provide access, the challenge, as Paul Rosenzweig has wisely pointed out, is that there is "growing body of [constitutional] law that protects encryption passwords against compulsory disclosure."[112] These cases, such as *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, make it difficult for law enforcement to decrypt data stored at rest even if authorities have lawfully seized the storage device and placed the suspect in custody, because they afford defendants a constitutional privilege, grounded in the Fifth Amendment's right against compelled self-incrimination, to not reveal passphrase to the private key or otherwise undertake decryption efforts when the government seeks compelled access to the underlying encrypted data.[113] In that case, as with others in various jurisdictions,[114] a panel of the Eleventh Circuit

---

110 *See* Rosenzweig, *Encryption, Biometrics*, *supra* note 72.

111 Sam Thielman, *FBI Head: Terror Fight Requires Open Backdoors to Encrypted User Data*, THE GUARDIAN (Dec. 9, 2015, 1:57 PM), http://bit.ly/1XXa65e.

112 *See* Rosenzweig, *Encryption, Biometrics, supra* note 72*; see also generally* Paul Rosenzweig, *Encryption Keys and Surveillance*, LAWFARE (Aug. 5, 2013, 2:00 PM) [hereinafter Rosenzweig, *Encryption Keys*], http://bit.ly/24SVKpS (explaining generally how Fourth and Fifth Amendment case law as interpreted issues relating to encryption).

113 *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

114 *See, e.g.*, *id.*; Sec. & Exch. Comm'n v. Huang, No. CV 15-269, 2015 WL 5611644, at*2-4 (E.D. Pa. Sept. 23, 2015).

> "We find, as the SEC is not seeking business records but Defendants' personal thought processes, Defendants may properly invoke their Fifth Amendment

held that the mandated decryption would be tantamount to compelled testimony because, like the required production of a defendant's knowledge of a combination to a safe—which the Supreme Court has strongly suggested is unconstitutional[115]—requiring decryption "use[s] [] the contents of [the defendant's] mind and…would be tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files."[116]

While there are admittedly some outs to this trick-box for the government—arguing, for example, that the existence of information sought by the govern-

---

right…The SEC argues any incriminating testimonial aspect to Defendants' production of the their personal passcodes already is a foregone conclusion because it can show Defendants were the sole users and possessors of their respective work-issued phones…SEC does not show the 'existence' of any requested documents actually existing on the smartphones. Merely possessing the smartphones is insufficient if the SEC cannot show what is actually on the device…Thus, the foregone conclusion doctrine is not applicable."

Id.; United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010).

"In this case, the government is not seeking documents or objects—it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password—that will be used to incriminate him…Accordingly, the Court quashes the subpoena requiring Defendant to testify—giving up his password—thereby protecting his invocation of his Fifth Amendment privilege against compelled self-incrimination."

Id.

[115] *See* Doe v. United States, 487 U.S. 201, 210 n. 9 (1988).

We do not disagree with the dissent that '[t]he expression of the contents of an individual's mind' is testimonial communication for purposes of the Fifth Amendment...We simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind. In our view, such compulsion is more like 'be[ing] forced to surrender a key to a strongbox containing incriminating documents' than it is like 'be[ing] compelled to reveal the combination to [petitioner's] wall safe.'

Id. (internal citations omitted); *Id.* at 219 (Stevens, J. dissenting).

A defendant can be compelled to produce material evidence that is incriminating. Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will. But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed.

Id.; *see also* United States v. Hubbell, 530 U.S. 27, 43 (2000) (holding the derivative use of produced documents unconstitutional because "[i]t was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents" similar to "telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.").

[116] *See In re* 2011 Grand Jury Subpoena, 670 F.3d at 1346.

ment was a "foregone conclusion"—cases like *In re: 2011 Grand Jury Subpoena* make clear that these solutions are narrow at best.[117] For example, in that case, the court determined that the government had not shown, nor argued that it knew whether the drives actually held any file nor that it knew, "with reasonable particularity[,] that [the defendant] is even capable of accessing the encrypted portions of the drives."[118] As a result, the court held that the government had not sustained its burden to show that the encrypted files actually existed, that the defendant had ongoing access to the evidence, nor could the government describe the evidence with reasonable particularity; therefore, the court held that the Fifth Amendment protected the defendant from having to decrypt the files for the government and reversed the district court's finding of contempt.[119]

Not all cases have turned out quite so poorly for the government, however. For example, *In re Boucher*, the government sought to compel a suspect to produce an unencrypted version of a drive on his laptop that was suspected to contain child pornography.[120] The judge denied the defendant's motion to suppress the subpoena based the fact that the government had previously inspected the relevant drive with the defendant's assistance and had determined that at least some of the files appeared to contain child pornography based on the contents of other file and the file names.[121] This, combined with the fact that the defendant had admitted to possession of the computer led the judge to determine that the government "thus [knew] of the existence and location of the Z drive and its files…[and] providing access to the unencrypted Z drive 'adds little or nothing to the sum total of the Government's information' about the existence and location of files that may contain incriminating information."[122] Other cases have, on occasion, suggested similar results, some even more favorable to the government.[123] At the end of the day, however, the weight of

---

117 *Id.* at 1346-53.
118 *See id.* at 1346.
119 *See id.* at 1346-53.
120 *See In re* Boucher, No. 2:06-MJ-91, 2009 WL 424718, at *3 (D.Vt. Feb. 19, 2009).
121 *See Id.* at *3-4.
122 *Id.* (citing Fisher v. United States, 425 U.S. 391, 411 (1976)).
123 *See, e.g.*, United States v. Gavegnano, 305 F. App'x. 954, 956 (4th Cir. 2009).

> "Gavegnano's Fifth Amendment claim, based on the fact that, after invoking his right to consult with an attorney, he was asked for, and revealed, the password to the computer, also fails. Any self-incriminating testimony that he may have provided by revealing the password was already a 'foregone conclusion' because the Government independently proved that Gavegnano was the sole user and possessor of the computer."

Id.; *but see* Huang, 2015 WL 5611644, at *3 (seeking to distinguish *Gavegnano* on the basis that "the Government could independently verify the defendant was the sole user and that he accessed child pornography websites because the computer was monitored for all activity.");

authority currently cuts strongly against the government being able to access to encrypted data even with a lawful court order due to the testimonial privilege, and those few cases in which the government has compelled production of a passcode are predicated on narrow exceptions that are unlikely to apply in the majority of cases, particularly fast-moving terrorism investigations.[124]

---

see also Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614-16 (2014).

> [W]e conclude that the factual statements that would be conveyed by the defendant's act of entering an encryption key in the computers are 'foregone conclusions' and, therefore, the act of decryption is not a testimonial communication that is protected by the Fifth Amendment…When considering the entirety of the defendant's interview with Trooper Johnson, it is apparent that the defendant was engaged in real estate transactions involving Baylor Holdings, that he used his computers to allegedly communicate with its purported owners, that the information on all of his computers pertaining to these transactions was encrypted, and that he had the ability to decrypt the files and documents. The facts that would be conveyed by the defendant through his act of decryption—his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key—already are known to the government and, thus, are a 'foregone conclusion.'…The Commonwealth's motion to compel decryption does not violate the defendant's rights under the Fifth Amendment because the defendant is only telling the government what it already knows.

Id.

[124] While the court in *Huang* distinguishes *Gavegnano* on the basis that an earlier part of the opinion in that case noted that *Gavegnano* was aware that the government was monitoring all traffic, it is far from clear that the court in *Gavegnano* relied on that fact to determine the applicability of the foregone conclusion doctrine. Indeed, to the contrary, the Fourth Circuit's citation to its earlier precedent in *United States v. Stone*, a case applying the foregone conclusion doctrine to utility bills belonging to a homeowner, militates in the opposite direction and suggests that, contrary to the holding in *Huang*, the Fourth Circuit may be willing to accept a government demonstration that an individual is the sole user and possessor of a given device in applying the foregone conclusion doctrine. *See* Huang, 2015 WL 5611644, at *3; *see* United States v. Stone, 976 F.2d 909, 911-12 (4th Cir.1992)*; see also Gavegnano,* 305 F. App'x at 956. At the same time, however, it is likely that the Eleventh Circuit's holding in *In re: 2011 Grand Jury Subpoena* and its reading of *Hubbell* as requiring government knowledge of some aspect of the evidence on a given device, rather than mere knowledge of sole possession and control of a device, is a more accurate reading of the case law as it stands today. *See In re*: *2011 Grand Jury Subpoena*, 670 F.3d at 1346-53; s*ee also Hubbell*, 530 U.S. at 35-36. As a result, it will be fairly difficult for the government to prevail other than in unique circumstances like those in *In re: Boucher*. *See In re Boucher*, No. 2:06-MJ-91, 2009 WL 424718, at *3-4 (D. Vt. Feb. 19, 2009). Note, however, that Prof. Orin Kerr has suggested for over a year now that another way out of this box for the government is to seek an order requiring a user to type in a password or passphrase, rather than provide the password or passphrase to the government. *See* Orin Kerr, *A Revised Approach To the Fifth Amendment and Obtaining Passcodes*, WASH. POST. (Sept. 25, 2015) http://wapo.st/1TFJUJO.

> [W]hen the government seeks a subpoena or order requiring the suspects to enter in their passcodes in a way that will unlock the phones…the government is seeking an act instead of testimony. The foregone conclusion doctrine should be satisfied and the order allowed when the government already knows that the person possessed the phone.

While it is true, as Rosenzweig points out, that the government may have other means to access such data, citing "black bag jobs" and espionage as two examples, he also correctly notes that putting encrypted data off limits from lawful court orders certainly serves to "weaken[] judicial control of law enforcement."[125] This, of course, is hardly a good result for those, like the framers, who believe the involvement of a neutral third party with life tenure is a foundational check on government action that serves as a robust protection for privacy.

Similar challenges exist with regard to government efforts to compel certain companies to provide government with the capability to access to the plaintext of their customer's encrypted data. As FBI Director Comey and Deputy Attorney General Sally Yates recently noted in joint testimony, the government faced a similar issue in the early 1990s with respect to wireline telephony tapping capabilities.[126] In response to that challenge, in 1994, Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA"), which requires "telecommunications carriers" to provide capabilities that allow the Government to intercept electronic communications—both content and metadata—when authorized by court order or other lawful process.[127]

At the same time, however, CALEA "does not require a carrier to decrypt communications encrypted by the customer unless the carrier provided the encryption and possesses the information necessary to decrypt."[128] Moreover, CALEA's historic focus on telecommunication carriers has meant that CALEA does not even reach "popular Internet-based communications services such as

---

Id.; Orin Kerr, *Virginia State Trial Court Ruling On the Fifth Amendment and Smart Phones*, WASH. POST. (Nov. 3, 2014) http://wapo.st/21Xi7ph.

> Because the passcode itself could be incriminating, the smart way to limit the Fifth Amendment problem is for the government to ask for an order compelling the target to enter in the passcode rather than to divulge it to the police….If the defendant has to enter in the passcode rather than tell it to the police, the testimonial aspect of complying would only be admitting knowledge of the passcode, which would very likely be a foregone conclusion in a case where the phone is used heavily by that person.

Id.

125 *See* Rosenzweig, *Encryption, Biometrics*, *supra* note 72.

126 *See Going Dark Hearing*, *supra* note 11, at 8.

> In the early 1990s, the telecommunications industry was undergoing a major transformation and the Government faced a similar problem: determining how best to ensure that law enforcement could reliably obtain evidence from emerging telecommunications networks. At that time, law enforcement agencies were experiencing a reduced ability to conduct intercepts of mobile voice communications as digital, switch-based telecommunications services grew in popularity.

Id.

127 *See id*.

128 *See id.*

email, Internet messaging, social networking sites, or peer-to-peer services," even though, over time, the Federal Communications Commission ("FCC") has extended CALEA's coverage "to include facilities-based broadband Internet access and Voice over Internet Protocol (["]VoIP["]) services that are fully interconnected with the public switched telephone network."[129] As a result, Comey and Yates argue, "the Government has lost ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA,"[130] which means that thousands of companies providing communications services are simply not covered by CALEA's requirements and, for such companies, "an order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper."[131]

This also means there is little incentive for voluntary cooperation—even if the major new technology companies, like Apple and Google, were even willing to provide it (which they are not). As Ben Wittes summarizes it:

The core of that emergent problem…is that CALEA—which mandates that telecommunications providers retain the capacity for law enforcement to get access to signal for lawful wiretapping—does not reach internet companies. So even if Apple and Google were to voluntarily retain encryption keys, some other actor would very likely not do so. Absent a legal requirement that companies refrain from making true end-to-end encrypted services available without a CALEA-like stop-gap, some entity will see a market hole and provide those services.[132]

To address these problems, FBI Director Comey has previously argued for "a regulatory or legislative fix to create a level playing field, so that all communication service providers are held to the same standard."[133] As we know, however, at this time, the White House has determined that the better path forward is not to seek legislative or regulatory authority but rather to work cooperatively with companies in the technology sector to determine whether other, voluntary solutions can effectively address the government's needs.[134]

PART IV: POTENTIAL PROPOSALS FOR CONSIDERATION

Having set out our basic arguments for why addressing this issue now is critically important, and having identified the key arguments on both sides of the encryption debate, along with some of the key legal issues, we seek to demonstrate to the reader that there actually some rational proposals out there

---

129 *Id*. at 8-9.
130 *Id*.
131 Comey, Brookings Institution Remarks, *supra* note 57.
132 Wittes, *Going Dark: Part I*, *supra* note 12.
133 Comey, Brookings Institution Remarks, *supra* note 57.
134 Perlroth & Sanger, *Obama Won't Seek Access, supra* note 18.

worth considering in the effort to find a middle ground. The goal in setting out the options below is not to support one proposal over another or to suggest that any one of these proposals is actually worth implementing. Rather, our goal is simply to demonstrate that even though each of these proposal is likely to be (or already has been) subject to a great deal of criticism from one side or the other, the fact that there are proposals that seek to bridge the gap between the two sides suggest that additional effort would be beneficial to further explore these proposals, and develop new ones, in search for a reasonable compromise. As we have previously suggested in this essay, our concern with the debate on these issues thus far is the absolutism and polarization in the arguments on both sides, which suggests an inflexibility and inability to reach an optimal outcome. Our concern, to make the core point yet once again, is that this dynamic, for which both sides deserve significant criticism, will almost certainly lead, in the long run, to an outcome that is both bad for national security and (particularly) bad for privacy and civil liberties in the long run. As a result, while we aren't doe-eyed about the challenges in making it happen, it is our hope that setting out these arguments might at least begin the conversation about how to actually bridge these gaps.

That being said, assuming the technology sector, advocacy groups, and the law enforcement and national security communities come to the table ready to work creatively and collaboratively, and ready to make tough choices and accept tough tradeoffs, to solve the encryption challenge, below are a few suggestions for how they might do so. Again, these suggestions are only meant to spur serious discussion; ultimately a solution will be identified only through serious and persistent dialogue among technologists, privacy experts, and counterterrorism officials.

Declassify Information relating to Terrorists' use of Encryption and the Impact of Encryption on Law Enforcement and Intelligence Efforts.

Among the chief problems that the law enforcement and national security communities face when trying to articulate the gravity of their concerns regarding the growing use by terrorists of encryption is to prove that it is in fact happening. This is the same basic concern that has plagued the national security community in trying to convince a skeptical public that its repeated warnings about the threat posed by terrorism is real and not simply an effort by government to scare the American public. While the attacks in Paris, San Bernardino, and Brussels suggest that the alarms sounded by government were legitimate, skeptics continue to argue that the government's claims that terrorists are using

encryption to plot terrorist attacks are unfounded and speculative.[135]

As our former colleague, Carrie Cordero, has wisely pointed out, it is critical that the government declassifies and makes public the facts underlying FBI Director Comey's claim that encryption presents real challenges to criminal prosecutions and protecting our national security.[136] To date, precious little detail has been provided by the FBI and, as Cordero notes, "[i]t will take more than a sampling of case anecdotes to make the case."[137] Cordero argues, correctly in our view, that the government should—as it did with CALEA in 1994—provide Congress and the public detailed statistics to make its case, and subjecting those claims to empirical testing by the Government Accountability Office and political testing on Capitol Hill.[138]

Undoubtedly declassifying such information will provide terrorist groups with additional information about what the U.S. government knows about their communications methodologies and platforms. As a result, it may very well serve to push them deeper underground and towards more secure and therefore harder to access technologies. However, given the importance of this issue, when combined with the scope and nature of the disclosures already made to date as a result of the Snowden leaks, in our view the government should seriously consider declassifying information—including a number of specific case studies—to help demonstrates terrorists' move to encryption following the Snowden disclosures as well as the use of American technology by these groups. Doing so would provide concrete data points for the American public—and American companies—in recognizing that terrorists are exploiting encryption to evade detection while they plot against the United States and are using the nation's infrastructure and technology, both at home and overseas, to do so.

Establish a Blue Ribbon Commission.

Many of the more specific proposals set forth below might usefully be considered by a bipartisan, blue ribbon commission composed of technologists, former government officials, security experts, privacy advocates, and other key stakeholders in an effort to reach consensus outside the normal policy and political processes. While such commissions admittedly have a checkered track record of actually achieving policy success, they have, on occasion, been able

---

135 Ryan Hagemann, *Encryption Was Not Responsible for the Paris Terrorist Attacks*, NISKANEN CTR. (Nov. 17, 2015), http://bit.ly/1QH8Vhw (considering the speculative nature of the connection between the Paris terrorist attacks and encryption).

136 Carrie Cordero, *Weighing in On the Encryption and "Going Dark" Debate*, LAWFARE (Dec. 4, 2014, 11:30 AM), http://bit.ly/1TFKhEq.

137 *Id.*

138 *Id.*

to demonstrate a solid consensus that, over time, might actually result in bipartisan legislation on Capitol Hill.[139] Indeed, Chairman of the House Homeland Security Committee Michael McCaul and Senator Mark Warner have recently called for the establishment of just such a commission, noting that "it is time to come together to confront these challenges."[140]

Encourage or Mandate the Use of Biometric Encryption.

Some academics and practitioners like Paul Rosenzweig and Herb Lin, one of the original authors of the 1990s National Academies of Science report on encryption, have suggested the use of biometric encryption, which uses a particular characteristic of the individual, such as their fingerprint, to generate a secure private key for use in encrypting their communications.[141] Such a scheme wouldn't build in any backdoors, but would instead require the use of what is likely a fairly secure method of protecting a private key.[142] At the same time, the use of such biometrically generated passcodes would enable law enforcement to obtain the access key with a court order from the target of the investigation using their biometrics—e.g., their fingerprint, which does not implicate the same testimonial Fifth Amendment concerns with seeking to compel an individual to verbally provide their passcode to law enforcement.[143] Of course, as Lin points out, these facts will not solve the concerns of the privacy community, who might also be worried that the widespread availability of

---

[139] Jordan Tama, *In Defense of Blue-Ribbon Commissions*, DEMOCRACY: A JOURNAL OF IDEAS (Apr. 20, 2011, 6:02 PM) http://bit.ly/1YoK1bR; Charles Blahous, *How to Run a Successful Commission (or Not)*, ECON. POL'Y FOR THE 21ST CENTURY (Dec 16, 2010), http://bit.ly/1pbPdnA; *see* Associated Press, *Panel Calls for New War Powers Legislation*, YOUTUBE (July 8, 2008) http://bit.ly/21XiwrN; *see generally* THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004).

[140] SEN. MICHAEL MCCAUL & SEN. MARK WARNER, MCCAUL – WARNER COMM'N ON DIG. SEC., THE CHALLENGE WE FACE 1 (2016), http://1.usa.gov/27wXHHp.

[141] Rosenzweig, *Encryption, Biometrics*, *supra* note 72; Herb Lin, *A Biometric Approach as a Partial Step Forward in the Encryption Debate*, LAWFARE (Dec. 3, 2015, 3:22 AM) [hereinafter Lin, *A Biometric Approach*], http://bit.ly/1R1tox1.

[142] Rosenzweig, *Encryption, Biometrics*, *supra* note 72.

[143] *Id.*

> Biometrics, unlike pass phrases, are almost certainly not protected by the Fifth Amendment. Hence the use of biometrics would restore the government's ability to secure evidence of criminality through lawful process….[and] access to data through a biometric would systematically be much more likely to be achieved by direct interaction with the subject of the investigation, restoring the notice aspect of data access that formerly had existed.

Id.; Lin, *A Biometric Approach*, *supra* note 141.

biometric samples, like fingerprints, could significantly reduce security.[144] In addition, Lin notes that the imprecision of some biometrics and the potential weakness of a given biometric-based key may create technological challenges to widespread use of biometrics for passcode generation.[145]

Differentiate Between Approaches to Data at Rest versus Data in Transit.

Many commentators have suggested that different rules regarding encryption may be appropriate for data at rest versus data in transit. Rosenzweig, for example, is less concerned with default data in transit encryption—and presumably law enforcement ought feel likewise—because "it conflicts with service provider business models."[146] The authors of the Harvard Berkman Center paper also note that many providers rely on access to user transmitted data to enable targeted advertising and thus satisfy their advertising revenue models, and as a result, are highly unlikely to put in place full, end-to-end encryption.[147] Given this, consensus may be more easily achieved if the relevant constituencies work to identify a workable approach for data at rest separate from efforts to identify a solution for data in transit rather than trying to address both in one fell swoop.

The "Try It Out" Approach.

Paul Rosenzweig suggested one rational approach to address the legitimate concerns of the advocacy groups that any provision for lawful access inherently makes the Internet fundamentally less secure could be to require that any proposal and methodology for providing lawful access be made available for public review and scrutiny for one year prior to implementation.[148] During that period, hackers, security professionals and the like would have the opportunity to stress test the proposal and methodology to determine whether it satisfies security and privacy concerns.[149] If so, and NIST judges it to have remained secure, then it would be implemented; if it were hacked, then the government would presumably go back to the drawing board.[150]

---

144 Lin, *A Biometric Approach*, *supra* note 141.
145 *Id.*
146 Rosenzweig, *Encryption, Biometrics*, *supra* note 72.
147 OLSON ET AL., *supra* note 99, at 10.
148 Paul Rosenzweig, *Testing Encryption Insecurity: A Modest Proposal*, LAWFARE (July 7, 2015, 4:48 PM), http://bit.ly/1LN7p0J.
149 *Id.*
150 *Id.*

Take Steps to Limit the Use of Non-Accessible Encryption Platforms.

Following the September 11 attacks, the U.S. government instituted a series of reforms, authorized under the USA PATRIOT Act, which require banks to adopt tighter 'know your customer' rules or face higher business costs and risk exclusion from the international banking system.[151] These regulations, enforced under authorities of the U.S. Treasury Department, had an immediate and significant impact on the ability of the government to kick terrorists off of the global financial network.[152] In much the same way as terrorists were previously exploiting the global financial system for terrorist financing purposes, they are now exploiting the global telecommunications system to communicate to recruit followers, incite them to violence, and plan attacks. Similar to the 'know your customer rules' enforced by Treasury, it may be possible to establish a program to 'designate' electronic communication service providers that refuse to enable a means for lawful government access to terrorist communications.[153] This program could then impose costs (both reputational and regulatory) on Internet 'backbone' companies if they permit communications from customers of designated providers to traverse their telecommunications infrastructure.[154] Such a program would enable the U.S. government to effectively drive encrypted terrorist communications off of the international communications grid, regardless of the jurisdiction in which the designated entity maintains its base of operations. In other words, the efficacy of such a regime is not tied solely to designated entities based in the United States. Moreover, this type of program would not require the creation of new surveillance authorities, but would instead restore the government's ability to gain access to terrorist communications under existing authorities. In addition, this type of program would not seek to impose specific technical requirements on encryption providers, though it would provide strong incentives for them to enable lawful government access in terrorism cases. Finally, if there is sufficient international interest in such a model (and to avoid concerns that the model is U.S. centric), it could be created and overseen internationally, perhaps through a model that resembles the international review mechanism in place under the Terrorist Finance Tracking Program.[155]

---

151 31 U.S.C. § 5311 (2012).

152 *See generally* Genci Bilali, *Know Your Customer - Or Not*, 43 U. TOL. L. REV. 319, 319 (2012).

153 *Id.* at 333.

154 Michael Kende, *The Digital Handshake: Connecting Internet Backbones*, 11 COMMLAW CONSPECTUS 45, 45 (2003) ("Internet backbones deliver data traffic to and from their customers.").

155 *Terrorist Finance Tracking Program (TFTP)*, U.S. DEP'T OF TREASURY (May 7, 2014, 10:24 AM), http://1.usa.gov/1J5eYJv.

Implement Device-Specific Front Doors.

Jonathan Alter has suggested that the government and technology community work together to develop a "device-specific 'front door' tech solution—a key that works only for that specific smartphone and can access only its contents."[156] Others, like the Manhattan District Attorney's office, have suggested a similar approach, such as mandating that all smartphones be able to be unlocked or accessed by the operating system designer, including by potentially prohibiting system designs that make such phones inaccessible to the government.[157] This approach would be similar to the situation with Apple iPhones prior to the introduction of iOS 8, where the government would provide Apple with a court order relating to a specific phone and Apple would use its own capabilities to access the encrypted data at rest on that specific device.[158] Alter also notes that in order to ensure that privacy was fully protected, new laws that limit the collection and use of information obtained from the authorized device may need to be put in place.[159]

Ensuring Lawful Access to Information Available to Companies for Business Purposes.

As mentioned above, the Berkman paper notes that a number of technology providers, like Google, earn revenue by accessing a significant amount of user information and content.[160] Because such providers will have access to the plaintext of otherwise encrypted data, the Berkman authors argue that the challenge posed to the government's by encryption can be mitigated by ensuring lawful access to the data the company accesses for its business purposes.[161] Underlining this point, as noted above, the Manhattan District Attorney's report indicates that many of the types of data available on an Android

---

156 Alter, *supra* note 79.

157 MANHATTAN D.A.'S REPORT, *supra* note 10, at 13.

> Federal legislation would provide in substance 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. Compliance with such a statute would not require new technology or costly adjustments. It would require, simply, that designers and makers of operating systems not design or build them to be impregnable to lawful governmental searches.

Id.

158 *See Legal Process Guidelines: U.S. Law Enforcement,* APPLE 3, 9 (Sept. 29, 2015), http://apple.co/1R3RUnm ("For iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a valid search warrant issued upon a showing of probable cause, Apple can extract certain categories of active data from passcode locked iOS devices.").

159 Alter, *supra* note 79.

160 OLSON ET AL., *supra* note 99, at 10.

161 *Id.* at 10-12.

smartphone may, under certain circumstances, be available in the Google Cloud.[162] Given this, one potential way to address the concerns posed by encryption could be to make companies like Google amenable to domestic process for their global stores of data and ensure that they have technical capabilities in place to provide access to the government pursuant to a lawful court order, at least to the extent that the data subject to such orders is data that the company accesses for its own business purposes. Such an effort could be accomplished through modest modifications to CALEA or through separate new statute.

Updating CALEA to Require Technical Bypass or Data Retention.

In a similar vein, Professor Orin Kerr has suggested adopting CALEA or E911 type regulations requiring manufacturers to have technical means to bypass smartphone passcodes or requiring data retention of specific types of data, including the content of, for example, text messages.[163] While Professor Kerr himself has since walked away from the former proposal[164] and the latter approach, long discussed as a potential option, has never really gained any serious traction, they are nevertheless additional options that policymakers and advocacy groups should explore further.

Implementing a Session Key Encapsulation and Key Splitting Approach for Private Escrow.

Some have also suggested a system requiring that service providers log pri-

---

162 *See* MANHATTAN D.A.'S REPORT, *supra* note 10, at 7.

163 Kerr, *Apple's Dangerous Game*, *supra* note 31. In the former article, Kerr also suggests that the government might raise penalties on the failure of an individual to employ their own passcode to access a smartphone. *Id*. This is in line with his view. *See* discussion *supra* note 124. We chose not to include this potential solution in our list of broad options because Prof. Kerr relies in significant part on *In re Boucher* and his own particular reading of earlier precedent for the proposition that imposing such a requirement would not contravene the Fifth Amendment's self-incrimination privilege. In our view, reading *Boucher* for this proposition is, at best, a stretch and would require some significant re-envisioning of the privilege against self-incrimination, at it is currently interpreted by the courts; more importantly, to our knowledge, the proposition has yet to be tested in adversarial litigation. *See, e.g.,* MANHATTAN D.A.'S REPORT, *supra* note 10, at 5 nn.15 & 17.

164 *See* Orin Kerr, *Apple's Dangerous Game, Part 2: The Strongest Counterargument*, WASH. POST, (Sept. 22, 2014), http://wapo.st/1W4qJXD ("[I]f Apple's longstanding backdoor works such that the government can't figure out physical access but hackers can use that backdoor to gain unauthorized remote access, then closing that backdoor adds a security benefit at the same time it imposes the unfortunate cost of thwarting valid warrants.").

vate session keys and split the key for preservation between several different entities.[165] Such a system—if it uses encapsulated and re-encrypted keys that are split amongst a number of private sector key holders employing an "M-of-N system" would address concerns regarding the creation of a single point of failure for exploitation in gaining access to decryption keys.[166] Under such a system, only one session at a time would be available per key pair recovered and the government would have to issue service of process to multiple private sector providers, M-of-N of whom would need to comply with (or could challenge) the government's request in order to recover each session key. Of course, like any key escrow system—even with its significantly heightened level of security born of key encapsulation and key splitting and the limited access it provides to a single session—this notional construct is likely to face serious challenges in the public debate, particularly given the resonance of the key escrow debate from the 1990s.[167]

Vet a Formal Proposal.

Dr. Herb Lin has suggested that the government propose a specific lawful access authority for public scrutiny and vetting, in order to enable robust con-

---

[165] *See, e.g.*, Rosenzweig, *Encryption Keys*, *supra* note 112.

> All of which suggests one possible business development would be for the providers to develop disposable one-time keys for each individual transmission, that they don't retain. My understanding from my technical friends is that this is currently theoretically possible, but difficult to implement on a large-scale basis. If, however, they want to retain customer confidence this may become a higher priority for some service providers.

Id.

[166] *See, e.g.*, Ellen Nakashima & Barton Gellman, *As Encryption Spreads, U.S. Grapples With Clash Between Privacy, Security*, WASH. POST (Apr. 10, 2015), http://wapo.st/1TnqdpI.

[167] *See* Matt Blaze, AT&T Bell Labs., Protocol Failure in the Escrowed Encryption Standard 1-2 (1994), http://bit.ly/1X8334I (explaining technical flaws in the Clipper chip that allowed a malicious user to evade the built in government decryption access to the Clipper system); Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES (June 12, 1994), http://nyti.ms/1RPhnhl.

> Employing normal cryptography, two parties can communicate in total privacy, with both of them using a digital "key" to encrypt and decipher the conversation or message. A potential eavesdropper has no key and therefore cannot understand the conversation or read the data transmission. But with Clipper, an additional key – created at the time the equipment is manufactured – is held by the Government in escrow. With a court-approved wiretap, an agency like the F.B.I. could listen in. By adding Clipper chips to telephones, we could have a system that assures communications will be private—from everybody but the Government.

Id.; *see generally* ANDI WILSON, DANIELLE KEHL & KEVIN BANKSTON, OPEN TECH. INST., DOOMED TO REPEAT HISTORY? LESSONS FROM THE CRYPTO WARS OF THE 1990S, at 5-11 (2015) http://bit.ly/1Svw8bm.

sideration and dialogue, in order to avoid the problem of both sides talking past one another.[168] In doing so, Dr. Lin proposes that the ensuing privacy and security debate focus on the anticipated time that it would take for the proposal to be compromised by cyber-attack.[169] Specifically, the question Lin proposes is whether the mean time to compromise is closer to one minute or 1000 years.[170] If one minute, the proposal should be abandoned; if 1000 years, the proposal should be strongly considered.[171] Dr. Lin believes that such a test would provide a measurable metric, supported by fact-based claims, which can be examined, tested, and verified to determine whether the government proposal should be pursued.[172] In Ben Wittes's view, this proposal does not align with the FBI's desires insofar as it asks the government to proffer a proposal, whereas the FBI:

> [W]ants to leave the development task to Silicon Valley to figure out how to implement government's requirements...[they] want[] to describe what [they] need[]—decrypted signal when [the FBI] has a warrant—and leave the companies to figure out how to deliver it while still providing secure communications in other circumstances to their customers.[173]

Regardless of whether it is government, the technology sector, or the two working together (which we think is the best approach), the core of Lin's proposal—that something concrete be put on the table—would still seem to provide a measurable and testable metric for the long-term security and efficacy of an approach to responsibly addressing the needs of law enforcement in an era of strong encryption.[174]

---

168 *See* Herb Lin, *Making Progress on the Encryption Debate*, LAWFARE (Feb. 24, 2015, 1:24 PM), http://bit.ly/1TnqtoM (arguing that the government should provide the private sector with an opportunity to independently test a proposed government-only access mechanism).

169 *Id.*

170 *Id*.

171 *See id.*

172 *See id.*

173 Ben Wittes, *Thoughts on Encryption and Going Dark, Part II: The Debate on the Merits*, LAWFARE (July 12, 2015, 2:00 PM) [hereinafter Wittes, *Going Dark: Part II*], http://bit.ly/1nslJQD.

174 *See id.*

Implement a Government Proposal through Vetting, Mandates, Liability Imposition, Letting Foreign Governments Take the Lead, or Waiting for a More Favorable Environment.

Wittes suggests five ways we might build off of Lin's general approach.[175] First, the government could start with a detailed "concept paper" that can be "evaluated, critiqued, and vetted."[176] Another option would be to simply require the industry, as a matter of law, to provide law enforcement access.[177] In Wittes's view, given market incentives, it is likely companies "will devote resources to the question of how to do so while still providing consumer security."[178] A third option would be to employ the potential for civil liability to incentivize companies to focus on these issues.[179] That is, one could create a (or take advantage of an existing) cause of action that allows damages to be recovered from a third party provider that is aware of the potential use of its systems by terrorists, with the expectation that the possibility of having to pay out will encourage companies to develop secure systems quickly.[180] A fourth approach would be to let other governments go first, likely China and the United Kingdom.[181] And a fifth and final approach is waiting for a shift in the situation on the ground; as Wittes notes,

If Comey is right and we start seeing law enforcement and intelligence agencies blind in investigating and preventing horrible crimes and significant threats, the pressure on the companies is going to shift […] Whereas the companies now feel intense pressure to assure customers that their data is safe from NSA […] In extraordinary circumstances, extraordinary access may well seem reasonable. And people will wonder why it doesn't exist.[182]

Overall, Wittes's view—and one that likely has significant merit—is that we ought pursue multiple lines of attack, including the proof of concept, civil liability reform, and continuing the political pressure.[183] While Wittes's construct is certainly helpful in understanding the various possible approaches to working through this problem, and while we are generally supportive of efforts along multiple fronts simultaneously, we strongly caution against a wait-and-see approach, which, as we have argued, would result in decisive action only in the aftermath of a catastrophic terrorist attack and would, as a result, have neg-

175 *See id.*
176 *See id.*
177 *See id.*
178 *See* Wittes, *Going Dark: Part II*, *supra* note 173.
179 *See id.*
180 *See id.*
181 *Id.*
182 *Id.*
183 *See generally id.*

ative consequences for both privacy and security.

Develop More Robust Endpoint Access and Adopt Related Policies.

Lin and others have also proposed that a fairly straightforward solution to the data in transit issue could be new authorities that enhance lawful government access to communication endpoints.[184] Some have argued that the government should actively exploit vulnerabilities it has knowledge of in order to obtain access to endpoints for the purpose of conducting properly authorized surveillance.[185] The challenge here, of course, is that the government doesn't have reliable and available access to communications endpoints for a number of reasons including the inaccessibility of overseas endpoints, and the time and resources that it takes to secure such access, time and resources that otherwise might be saved if the government had access to the relevant data in transit, particularly through a provider where multiple endpoints, such as burner phones or email accounts, may be surveilled under a single order. As proponents of this approach rightfully note, this form of "lawful hacking" presents unique challenges beyond sporadic access and unreliability, including concerns regarding government exploitation of identified vulnerabilities rather than taking steps to publicly acknowledge these vulnerabilities and assist the private sector in addressing them, and the potential reputational damage to U.S. companies if they are perceived as working with the government on a voluntary, rather than compulsory, basis. [186] The resolution to the former problem, according to the proponents of lawful hacking is immediate reporting by the government except in exceptional cases; according to these authors, given patch development, patching inconsistency, and the relatively high number of potential vulnerabili-

---

[184] *See, e.g.*, Herb Lin, *Another Take on the Lessons of Paris Shootings for Encryption*, LAWFARE (Nov. 27, 2015, 1:14 PM), http://bit.ly/1U8Qfff.

> Encrypted communications must be decrypted and displayed for the terrorist or criminal to read them, and thus they can be captured by on-device software. Message capturing software could be pushed only to individuals under suspicion (and only with appropriate legal oversight). In principle, there is no reason that government authorities could not read encrypted terrorist communications a few moments after the terrorist read them.

Id.

[185] *See, e.g.*, Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 24-44 (2014); *see also* Susan Landau, *Thoughts on Encryption and Going Dark: Counterpart*, LAWFARE (July 15, 2015, 3:27 PM), http://bit.ly/1TnqN73 ("Devices — laptops, phones, any object running complex software — have flaws. When there are such vulnerabilities, there is room for attack, for downloading a wiretap against the device and tapping the communications *before* those communications are encrypted.").

[186] *See* Bellovin et al., *supra* note 185, at 47-48.

ties available, the government's ability to obtain communications should not be significantly compromised.[187] In reality, however, top-notch capabilities often look to exploit relatively narrow vulnerabilities—including zero days[188]—that are few and far between in particular systems. That is, simply saying that a large number of vulnerabilities exist and that immediate reporting and patching won't slow the government down doesn't make it so. Of course, there is much to be said about the relative tradeoffs here[189] and there is significant merit to the argument that if the government is able to significantly strengthen its abilities to obtain endpoint access, both in terms of laws and capabilities, such advances could mitigate some reasonable aspect of the encryption challenge.

PART V: CONCLUSION

Despite the urgency of the problem, the government has done little to restore its ability to gain access to terrorist communications. No doubt the technological issues posed by encryption are extremely complex,[190] and there may be no silver bullet. Yet to a significant degree, the government's failure to act decisively is the direct result of voices, both from within the government and from the tech sector and advocacy organizations,[191] which would simultaneously claim technological impossibility while decrying government efforts to enhance its law enforcement and national security tools. The hyperbolic policy arguments that any such enhancements necessarily entail a heightened risk of government abuse and hegemony, and that any solution that enables government access to terrorist communications would also result in the degradation of the availability of strong encryption to promote internet freedom and privacy,

---

187 *See id.* at 52-53.

188 Kim Zetter, *Hacker Lexicon: What Is a Zero Day?*, WIRED (Nov. 11, 2014, 6:30 AM) http://bit.ly/1QyOyp3.

> Zero-day vulnerability refers to a security hole in software—such as browser software or operating system software—that is yet unknown to the software maker or to antivirus vendors. This means the vulnerability is also not yet publicly known, though it may already be known by attackers who are quietly exploiting it. […] Zero-day exploit refers to code that attackers use to take advantage of a zero-day vulnerability.

Id.

189 Marshall Erwin, *The High Standard of Proof in the Encryption Debate*, JUST SEC. (Feb. 5, 2016, 9:35 AM), http://bit.ly/24MWgn1.

190 Matt Blaze, *A Key Under the Doormat Isn't Safe. Neither Is An Encryption Backdoor,* WASH. POST (Dec. 15, 2015), http://wapo.st/1QCLKsc ("Despite many advances in computer science, building a secure access feature is actually harder now than it was when Clipper failed in the 1990s. This is partly because we now rely on encryption integrated deeply into systems that are more complex, and fragile, than ever.").

191 Alex Abdo, *ACLU to UN: Encryption is Not A Problem to be Solved, But a Crucial Tool For Freedom and Security*, AM. CIV. LIBERTIES UNION (Feb. 11, 2015, 10:56 AM), http://bit.ly/1pbQlYz.

for example, for dissidents who want to speak out about repressive regimes have had a polarizing effect on the debate.

While there is no doubt there are very real tradeoffs between privacy and security, particularly for those defending the values of freedom and liberty overseas, the conflation of factual impossibility with policy claims regarding such trade-offs strangles any form of real discussion. In our view, it is inappropriate to allow the policy debate over the value of such trade-offs to be held hostage by continuing claims of technological impossibility, a claim that is fundamentally at war with the thousands of years of human ingenuity and technological innovation; innovation that has often solved major problems once thought intractable.

As a result, while the arguments and rhetoric surrounding the current challenges and virtues of encryption should be fully explored as part of a broader engagement on terrorist use of the Internet, but they cannot be allowed to frighten policymakers from finding a solution. The need to shore up defenses from terrorism demands a solution. If the attacks in Paris occurred in New York City, or if the United States face another major terrorist attack on its soil, the American public will demand a solution. The pendulum will swing back to national security. And in the frantic efforts to find a solution at all costs, privacy and free Internet concerns will take a back seat to the needs of the law enforcement and national security communities. Sadly, this is expected to be an inevitability given ISIL's and al-Qaida's determination to strike the U.S. homeland, and given our diminished ability to thwart them.

In our view, security and privacy are best served by finding common ground on the encryption matter now, in the relative calm, rather waiting to act in the aftermath of an attack when security will already have been sacrificed and privacy will pay a significant long term cost.

For this reason, the tech sector and advocacy groups should be incentivized to come to the negotiating table now, and help law enforcement and the national security community acquire the tools they need to re-establish insights into terrorist plotting, under a regime sensitive to privacy and free internet concerns. We've set out a number of potential proposals that might be considered during such a group negotiation. In particular, two proposals that deserves serious consideration now is the declassification of information related to terrorists use of American providers and encryption and the creation of a blue ribbon panel to vet some of the proposals mentioned above as well as others. Given the threat we face and the very real challenges posed both to national security and privacy, inaction and policy incrementalism or policy creep are not valid approaches to address this issue. As such, we stand ready to support our friends and colleagues on both sides of the aisle as we come together to address this

difficult and pressing issue.