UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 17 | Issue 4 Article 3

5-1-2016

You Can't Always Get What You Want: How Will Law Enforcement Get What it Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?

Stephanie K. Pell

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 17, ISSUE 4: MAY 2016

YOU CAN'T ALWAYS GET WHAT YOU WANT: HOW WILL LAW ENFORCEMENT GET WHAT IT NEEDS IN A POST-CALEA, CYBERSECURITY-CENTRIC ENCRYPTION ERA?

Stephanie K. Pell*

In recent years, many technology companies have enabled encryption by default in their products, thereby burdening law enforcement efforts to intercept communications content or access data stored on smartphones by traditional means. Even before such encryption technologies were widely used, however, the Federal Bureau of Investigation ("FBI") claimed its surveillance capabilities were "Going Dark" due to the adoption by consumers of new IP-based communication technologies, many of which are not subject to any surveillance-enabling obligations under the Communications Assistance for Law Enforcement Act ("CALEA"). The heightened tension produced by the introduction of encryption by default into an environment where terrorism has magnified the need for efficient law enforcement access (surveillance) supported by a newly-expanded CALEA framework is often framed as a contest between privacy and security. It is, however, more accurately framed as a security issue on both sides, one side which integrates traditional privacy concerns with the growing focus upon cybersecurity equities (the "cybersecurity" argument) into a critique of a second regime of "exceptional access" posited by law

* Assistant Professor & Cyber Ethics Fellow, Army Cyber Institute & Department of English and Philosophy, United States Military Academy at West Point; Affiliate Scholar Stanford Law School's Center for Internet and Society; email: stephanie@stephaniepell.net.

I would like to thank Professor Anne Klinefelter and the NC JOLT staff members for inviting me to participate in 2016 NC JOLT Symposium and publish in the corresponding Symposium issue of NC JOLT. I would also like to thank Steve Bellovin, Jim Green, Andrea Matwyshyn, and Chris Soghoian for their feedback and assistance. The views represented here are the author's views and do not reflect the position of the United States Military Academy at West Point, the Army, or the United States Government.

enforcement to sustain its access advantages either: (1) by mandating that manufacturers insert "backdoors" into applications, devices and communications networks; or (2) by forcing companies, after-the-fact, to circumvent and undermine security features they purposefully build into their products and services. The cybersecurity and, incidentally, pro-privacy position rejects exceptional access as a dangerous fiction that would, among other things, create new attack surfaces, rendering networks more vulnerable to every form of predation, from financial crime and IP theft to cyber espionage, ultimately generating unacceptable risks to our national and economic security. The reconciliation of these competing visions of security—of law enforcement's traditional public safety mission with cybersecurity—will require law enforcement to employ investigative techniques that may include, among other things, enhanced collection and exploitation of metadata, which is not generally thwarted by the use of encryption technology. Although many sources and forms of metadata are already available to law enforcement, the widespread adoption of Internet of Things ("IoT") technology will generate additional forms of metadata, potentially revealing sensitive information that would have been difficult for the government to obtain in the past. Moreover, many IoT devices include microphones and cameras that could be used to eavesdrop remotely on targets, whether through direct hacking or through law enforcement's power to compel third parties to facilitate such eavesdropping, thereby potentially mitigating surveillance losses due to a target's use of encrypted communications.

This Article asserts that, for better or worse, law enforcement has entered a new post-CALEA, cybersecurity-centric investigative era where the use of encryption and other security-enhancing technologies is an irreversible fact and where getting a warrant or court order will not, in and of itself, guarantee law enforcement access to communications data. In this new surveillance era, law enforcement will more often find itself forced to employ individualized "collection" solutions for specific investigations, rather than enjoy the ready-made access provided by a CALEA-like regime. That is, law enforcement will need, among other

things, to target end-point devices, such as phones, computers and IoT devices, rather than the surveillance mechanisms mandated by a CALEA-like regime. As law enforcement seeks to employ old and new kinds of investigative techniques that involve neither designing access points into communications networks nor mandating circumvention of security features in mobile devices—policy choices necessary to support fundamental imperatives of cybersecurity—policy makers will be forced to consider how to facilitate, regulate, and oversee these law enforcement capabilities and activities, balancing what law enforcement may need against the social benefits of transparency and electronic privacy. The current debate over law enforcement exceptional access is more consistently divisive than not and, for the most part, not focused on how to get law enforcement what it needs without undermining fundamental principles of cybersecurity. A new dialogue on how to get law enforcement what it actually needs in a Post-CALEA, default-encryption era would be a much-needed step forward. That journey forward, however, will require a return to some of the historical debates about metadata collection and standards governing law enforcement access to various kinds of new revelatory metadata, such as that generated through the ever-expanding IoT. Moreover, this journey will raise new legal, ethical, and policy questions about when and if law enforcement should be permitted to use IoT apertures for seeing and hearing activities inside the home.

TABLE OF CONTENTS

I. INTRODUCTION

It all started with a very small, unremarkable moment in time. In July of 1999, a constable from the Warwickshire Constabulary was awakened in the middle of the night and informed about a package judged to be suspicious by an x-ray technician at Coventry Airport in Coventry, England.[1] The package contained a .357 Magnum revolver hidden inside a child's toy boat.[2] In the coming days and weeks, more packages containing weapons and ammunition concealed inside children's toys and hollowed-out computer towers were discovered at Coventry airport, as well as airports and post offices up and down the East Coast of the United States, where they were intercepted en route to destinations overseas.[3] Agents noticed that the serial number on the revolver from the first package had been filed down but forensic analysts reconstructed the number, which allowed law enforcement to trace the gun back to a dealer in South Florida and, subsequently, to a woman who had purchased it there.[4] Moreover, the first group of packages discovered at the Coventry airport was mailed from South Florida via Express Mail, which allowed agents to identify the locations, times, and dates on which each package was mailed.[5] Cameras inside those post offices recorded video showing two men mailing the first package containing the .357 Magnum.[6]

A comprehensive, labor-intensive investigation ensued.[7] Federal agents obtained and reviewed express mail mailing records, driver's license records, financial records, and forms

---

[1] This factual scenario is taken from a real case prosecuted by the author of this Article in 1999–2000. United States v. Claxton, No. 99-06176 (S.D. Fla. June 13, 2000) (Ferguson, J.). For more information about the case, *see* Mike Clary, *Lax Florida Laws Attracted IRA*, REGISTER-GUARD, June 8, 2000, at 6A, https://news.google.com/newspapers?id=ilNWAAAAIBAJ&sjid=hOsDAAAAIBAJ&pg=6729%2C2038072.

[2] United States v. Claxton, *supra* note 1.

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

documenting the purchase of firearms.[8] They also conducted physical surveillance by car and on foot, executed search warrants on places where the defendants lived, and performed various kinds of forensic analysis, among other investigative techniques, that notably *did not* involve the interception of communications content.[9] These efforts identified four individuals who were arrested, then indicted on various terrorism and gun smuggling charges.[10] Ultimately, the investigation revealed these defendants were part of a cell of Irish Republican Army ("IRA") operatives who came to the United States, purchased weapons illegally, hid them in children's toys and hollowed-out computer towers, and mailed them to the Republic of Ireland, where they were to be smuggled into Belfast.[11] This operation continued unabated during a critical time in the peace process. The weapons were intended to replace surreptitiously the cache of weapons being publicly turned over as part of the Good Friday Agreements.[12] The "Troubles"[13] found their way to South Florida, and it took an exhaustive effort by FBI Miami's Joint Terrorism Task Force, working with agents in other parts of the country and with foreign partners, to identify the individuals involved in and, ultimately, to disrupt this gun-running operation.[14]

This condensed factual narrative describing a case the author of this article investigated and prosecuted only sixteen years ago, in 1999–2000, is a useful historical template for analysis of some of the critical discourse about current law enforcement investigative capabilities. The IRA case, a pre-September 11th terrorism investigation, occurred before the advent and ubiquitous adoption

---

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *See The Troubles*, BBC, http://www.bbc.co.uk/history/troubles ("The Troubles refers to a violent thirty year conflict framed by a civil rights march in Londonderry on 5 October 1968 and the Good Friday Agreement on 10 April 1998. At the heart of the conflict lay the constitutional status of Northern Ireland.").
[14] *See* United States v. Claxton, *supra* note 1.

of smart phones, thus none of the rich metadata and tracking capabilities currently provided by modern mobile devices was available to the IRA case investigators. Indeed, while some of the IRA defendants were discovered to have had cell phones, these phones were not useful sources of information during the course of the investigation.[15] In fact, no phone conversations or other forms of communications content were ever intercepted by law enforcement.[16] On the day agents planned to arrest all of the defendants, for example, one defendant evaded law enforcement's physical surveillance of him and drove all the way from South Florida to Philadelphia, where he was later located and arrested without the aid of location data produced by a cellular phone.[17] The most useful oral statements by any defendant did not come as a result of wiretaps, but through a Mirandized confession of the lead defendant, Conor Claxton, who told agents that this was a Provisional Irish Republican Army operation, that the peace process was not working, and that the weapons were meant to kill British police and Protestant paramilitary forces.[18]

One current heated public discussion pertaining to law enforcement's allegedly waning surveillance capabilities is generally referred to as the "Going Dark" debate, one aspect of which is commonly alluded to as the current "Crypto Wars." This debate springs from claims by high-level law enforcement officials, including the FBI Director[19] and the Manhattan District

---

[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *See generally* Statement of James Comey, Director of the Federal Bureau of Investigation, Before the House Judiciary Committee Hearing *Encryption Tightrope: Balancing Americans' Security and Privac*y, FBI, (Mar. 1, 2016), *available at* https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy ("When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads we may not be able to root out the child predators hiding in the shadows of the Internet or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not

Attorney,[20] that law enforcement no longer has sufficient access to evidence and information necessary to fulfill its traditional public safety mission including, among other things, preventing terrorist attacks, locating kidnapped children, and apprehending pedophiles. The basis of this claim stems primarily from three recent burdens placed upon law enforcement's access to communications data: (1) the default encryption of smartphone data using technology that prevents the phone manufacturer from being able to access it and turn it over to law enforcement, even in response to a warrant;[21] (2) the protection of voice, video, and text communications with end-to-end encryption where communication service providers do not have access to the encryption keys, thereby preventing them and, consequently, law enforcement from getting access to unencrypted communications;[22] and (3) the consumer adoption of IP-based communications services that, while not employing end-to-end encryption, nevertheless do not fall under the Communications Assistance for Law Enforcement Act's ("CALEA")[23] mandate requiring service providers to provision their networks in a way that will enable law enforcement wiretapping capabilities (without

---

be able to recover critical information from a device that belongs to a victim who cannot provide us with the password especially when time is of the essence. These are not just theoretical concerns."). *Id*.

[20] *See generally* REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE, ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY, (Nov. 2015) [hereinafter Manhattan DA report]. "Apple's and Google's decisions to enable full-disk encryption by default on smartphones means that law enforcement officials can no longer access evidence of crimes stored on smartphones, *even though the officials have a search warrant issued by a neutral judge*. *Id*. at i (emphasis in original).

[21] *Id.*; *see infra* discussion Part II.

[22] *See infra* discussion Part II.

[23] 47 U.S.C. §§ 1001–1010 (2006). CALEA was enacted "to ensure that law enforcement surveillance capabilities remained intact during the move from a copper-wire phone system to digital networks." Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 421 (2012). CALEA did not, however, require a telecommunications carrier to be capable of decrypting communications that were encrypted by a subscriber or customer unless the carrier "provided the encryption" and "possessed the information necessary to decrypt the communication." 47 U.S.C. §1002(b)(3).

such purposeful provisioning, communications data may not be available to law enforcement).[24]

While federal law enforcement agencies have not proposed new, specific legislative language to mandate access to new communications technologies,[25] they have called for companies to create "backdoors"[26] that will provide law enforcement access to

[24] *See infra* discussion Part II. Federal Communications Commission (FCC) Chairman Tom Wheeler discussed the need to expand CALEA when it was believed that Islamic State perpetrators of the Paris terrorist attacks communicated using the Playstation 3 video game chat function (an IP-based communications service not covered by CALEA's wiretapping mandate). Brian Fung and Andrea Peterson, *FCC Chairman Suggests Expanded Wiretap Laws in Response to the Paris Attacks*, WASHINGTON POST (Nov. 17, 2015), *available at* https://www.washingtonpost.com/news/the-switch/wp/2015/11/17/the-fcc-suggests-expanded-wiretap-laws-in-response-to-the-paris-attacks/.

[25] As of the writing of this Article, the Administration has indicated that it would not seek legislation to require companies to provide access to encrypted communications, although the FBI Director continues to "pres[s] companies for special government access." Nicole Perloth and David E. Sanger, *Obama Won't Seek Access to Encrypted Data*, Oct. 10, 2015, http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html. Senators Feinstein and Burr have, however, released a discussion draft of a bill, called the "Compliance With Court Orders Act of 2016, that would require companies to render unintelligible data intelligible. *See* Andy Greenberg, *The Senate's Draft Encryption Bill is Ludicrous, Dangerous, Technically Illiterate*, WIRED (April 8, 2016), http://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/ ("[T]he bill would make illegal the sort of user-controlled encryption that's in every modern iPhone, in all billion devices that run Whatsapp's messaging service, and in dozens of other tech products. 'This basically outlaws end-to-end encryption,' says Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology. 'It's effectively the most anti-crypto bill of all anti-crypto bills.'"). *Id*. *See also* Riana Pfekkerkorn, *Here's What the Burr-Feinstein Anti-Crypto Bill Gets Wrong*, JUST SECURITY (April 15, 2016), https://www.justsecurity.org/30606/burr-feinstein-crypto-bill-terrible/. For an explanation of end-to-end encryption, *see infra* note 27.

[26] *See* David Kravets, *FBI Chief Tells Senate Committee We're Doomed Without Crypto Backdoors*, Ars Technica (Jul. 8, 2015) http://arstechnica.com/tech-policy/2015/07/fbi-chief-tells-senate-committee-were-doomed-without-crypto-backdoors/ ("James Comey, the director of the FBI, told a Senate committee Wednesday that the government should have the right to lawfully access any device or electronic form of communication with a

this information, including data "in motion" that is encrypted end-to-end.[27] The problem with this "request" and any legal mandate that might develop from it is that there are no "one way" backdoors available exclusively to law enforcement. Indeed, security experts warn that this notion of law enforcement "exceptional access" is a dangerous fiction that threatens to undermine our national and economic security.[28] As Professor Matt Blaze, cryptographer, computer scientist, and security researcher explained in written testimony prepared for a congressional hearing on encryption technology and possible policy responses:

> At first blush, a "lawful access only" mechanism that could be incorporated into the communications systems used by criminal suspects might seem like an ideal technical solution to a difficult policy problem. Unfortunately, harsh technical realities make such an ideal solution effectively impossible, and attempts to mandate one would do enormous harm to the security and reliability of our nation's infrastructure, the future of our innovation economy, and our national security.[29]

---

lawful court order, even if it is encrypted. Comey and another Justice Department official briefed the Senate Judiciary Committee and complained that keys necessary to decrypt communications and electronic devices often reside 'solely in the hands of the end user'—which they said is emblematic of the so-called 'Going Dark problem.' Companies should bake encryption backdoors into their products to allow lawful access, they said.").

[27] End-to-end encryption can be generally described as "a method to secure data while in flight from one device to another . . . [and] loosely define[d] as a method to protect data in flight over a network such that only each end of the transaction has the ability to see the plaintext." Branden Williams, WILL END TO END ENCRYPTION SAVE US ALL?, 3 (2010), *available at* https://www.brandenwilliams.com/brwpubs/WillEndtoEndEncryptionSaveUsAll.pdf.

[28] *See* Steven Bellovin, *The Danger of Exceptional Access*, CNN OPINION (Nov. 18, 2015), http://www.cnn.com/2015/11/18/opinions/bellovin-encryption-debate/("It would be nice if we could safely and effectively change our cryptography to let us spy on the bad guys. Unfortunately, we can't. So if we insist on systems that allow exceptional access, we end up weakening our own security without enhancing our ability to monitor them. And in the process, we may just make it easier for terrorists to exploit weakened cryptosystems -- and do us more harm in the process.").

[29] *Encryption Technology and Potential U.S. Policy Responses: Hearing Before the Subcomm. on Infor. Tech. of the H. Comm. on Oversight and Gov't*

Reform, 114th Cong. 3-4 (2015) (written testimony of Professor Matt Blaze) https://oversight.house.gov/hearing/encryption-technology-and-potential-u-s-policy-responses/ [hereinafter Blaze]; *see also,* HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS 1–3 (2015), https://dspace.mit.edu/bitstream/handle/1721.1/ 97690/MIT-CSAIL-TR-2015-026.pdf ("As computer scientists with extensive security and systems experience, we believe that law enforcement has failed to account for the risks inherent in exceptional access systems . . . . There are three general problems. First, providing exceptional access to communications would force a U-turn from the best practices now being deployed to make the Internet more secure. These practices include forward secrecy — where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications. A related technique, authenticated encryption, uses the same temporary key to guarantee confidentiality and to verify that the message has not been forged or tampered with. Second, building 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. This is a far more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services, which tend to use similar technologies and are more likely to have the resources to manage vulnerabilities that may arise from new features. 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. Third, exceptional access would create concentrated targets that could attract bad actors. Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. If law enforcement's keys guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege. Moreover, law enforcement's stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple keyholders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the United States Government Office of Personnel Management (OPM) show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities. In the case of OPM, numerous federal agencies lost sensitive data because OPM had insecure infrastructure. If service providers implement exceptional access requirements incorrectly, the security of all of their users will be at risk.")

As part of the analysis supporting this assertion, Professor Blaze explains that modern digital systems are extremely vulnerable because computer science "does not know how to build complex, large-scale software that has reliably correct behavior."[30] He goes on to describe the observed effects of increasing complexity in software systems upon their relative security:

> The number of software defects in a system typically increases at a rate far greater than the amount of code added to it. So adding new features to a system that makes it twice as large generally has the effect of making it far more than twice as vulnerable. This is because each new software component or feature operates not just in isolation, but potentially interacts with everything else in the system, sometimes in unexpected ways that can be exploited. Therefore, smaller and simpler systems are almost always more secure and reliable, and best practices in security favor systems [with] the most limited functionality possible. The goal is to minimize the "attack surface"[31] that any software vulnerabilities would expose.[32]

A backdoor, a general term describing a mechanism or access point in a communications device or network that enables "the creator of software or hardware [to] access data without the permission or knowledge of the user,"[33] creates an additional attack surface.[34] Specifically, code must be written to create the backdoor and the code must have unfettered access to communications content.[35] The additional code creates the potential for more bugs (more code, more bugs) that could be exploited to allow improper access to the system.[36] Moreover, for a backdoor in an encrypted

---

[30] Blaze, *supra* note 29, at 2.

[31] For more about "attack surfaces," *see* Pravetz, *infra* note 34.

[32] Blaze, *supra* note 29, at 3.

[33] Swire & Ahmad, *supra* note 23, at 460.

[34] Jim Pravetz, *What's An Attack Surface?*, THE ZERO TOUCH BLOG (Feb. 23, 2013), http://www.armor5.com/blog/2013/what-is-attack-surface/ ("In the world of computer security, the term *attack surface* refers to the depth of methods a hacker can use to exploit your system.").

[35] Interview with Dr. Christopher Soghoian (Mar. 28, 2016). For more information about Dr. Soghoian's background see https://www.dubfire.net/.

[36] *See* Blaze, *supra* note 29, at 3. *See also* Chad Perrin, *The Danger of Complexity: More Code, More Bugs*, IT SECURITY BLOG (Feb. 2, 2010), http://www.techrepublic.com/blog/security/the-danger-of-complexity-more-code-more-bugs/3076 ("If you want to produce secure software you should

communications service to offer interception functionality, the service provider must have momentary access to the unencrypted communications data.[37] As a result, if and when security flaws in the system are discovered and exploited, the worst-case scenario will be unauthorized access to users' communications.[38] In other words, when compromised, an encrypted communications system with a lawful interception backdoor is far more likely to result in the catastrophic loss of communications confidentiality than a system that includes no capability allowing deliberate access to the unencrypted communications of its users.[39]

The recent high-profile dispute between Apple and the FBI over the FBI's inability to access data on an iPhone used by one of

---

focus on following the advice. All else being equal if you can find a way to eliminate lines of code without compromising the proper functioning of the software you will probably improve the security of the software substantially.").

[37] Interview with Dr. Christopher Soghoian, (Mar. 28, 2016).

[38] *Id.*; *see also Storing Passwords, or The Risk of a No-Salt Diet*, TECH@FTC (Mar. 21, 2013), http://techatftc.wordpress.com/2013/03/21/storing-passwords-or-the-risk-of-a-no-salt-diet/. When discussing best practices for storing and protecting passwords, security researcher Dr. Steven Bellovin begins with a fundamental security principle: "It's a prime rule of security: something that doesn't exist can't be stolen. Conversely, if something does exist, it can be stolen or leaked in many, many ways." *Id.* This principle is applicable to law enforcement backdoors as well: If they exist, they will be discovered and exploited; *see also* Bellovin, *supra* note 28.

[39] Interview with Dr. Christopher Soghoian, (Mar. 28, 2016). Researchers Micah Sheer, Eric Cronin, Sandy Clark, and Matt Blaze have done research illustrating ways to exploit wiretapping technology. *See Signaling Vulnerabilities in Wiretapping* Systems (Nov. 2005), http://www.computer.org/csdl/mags/sp/2005/ 06/j6013-abs.html. Moreover, information revealing U.S. government targets of interception in the possession of third parties can prove to be an irresistible target for China. *See* Matthew J. Swartz, *Google Aurora Hack Was Chinese Counterespionage Operation*. Information Week Dark Reading (May 21, 2013) http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060. ("Former government officials with knowledge of the breach said attackers successfully accessed a database that flagged Gmail accounts marked for court-ordered wiretaps. Such information would have given attackers insight into active investigations being conducted by the FBI and other law enforcement agencies that involved undercover Chinese operatives."). *Id.*

the San Bernardino shooters[40] has further elevated and exposed tensions between the FBI and Silicon Valley over the decision, by some companies, to include strong encryption and other cybersecurity technologies in their products.[41] At issue is the fact that, starting with iOS 8, Apple's mobile devices encrypt user data, by default, with a key that is inaccessible to Apple.[42] Earlier versions of Apple's operating system had encrypted the data with a key that remained accessible to Apple and, as a result, the company could extract data from seized devices for law

---

[40] *See In the Matter of the Search of An Apple iPhone Seized During the Execution of a Search Warrant on A Black Lexus IS300, California License Plate 35KGD203*; Government's Ex Parte Application For Order Compelling Apple Inc. to Assist Agents in Search; Memorandum of Points and Authorities; Declaration of Christopher Pluhar; Exhibit (Feb. 16, 2016) (Central District of California ED No. 15-0451M) (hereinafter "Government's Ex Parte Application For Order Compelling Apple"). At the time the government filed this Motion to Compel Apple's assistance to unlock the iPhone, the government claimed that it was unable to access the encrypted content on the phone and that "Apple has the exclusive technical means which would assist the government in completing its search but has declined to provide that assistance voluntarily." *Id*. at 3. Since that time, third party professional hackers have assisted the government with getting access to the encrypted data on the phone, *see infra* note 52. *See* Kevin Johnson, Jon Swartz and Marco della Cava, *FBI Hack's Into Terrorist's iPhone Without Apple*, USA Today (Mar. 29, 2016) http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-farook/82354040/. The government has, therefore, requested that the original order compelling Apple's assistance be vacated. See *In the Matter of the Search of An Apple iPhone Seized During the Execution of a Search Warrant on A Black Lexus IS300, California License Plate 35KGD203;* Government's Status Report (Mar. 18, 2016).

[41] In reaction to this high-profile case, the House Judiciary Committee held a hearing to examine the matter (witnesses included the FBI Director, Apple's General Counsel and the Manhattan DA); *see* https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy/. More colloquially, John Oliver presented a recent satiric piece on the FBI vs. Apple fight; *see* John Oliver, *Last Week Tonight with John Oliver: Encryption (HBO)*, LAST WEEK TONIGHT, (Mar. 13, 2016), https://www.youtube.com/watch?v=zsjZ2r9Ygzw.

[42] *See* Apple's Process Guidelines at 9, US Law Enforcement ("For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions as data extraction tools are no longer effective. The files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."). *Id.* at 9.

enforcement.[43] In the case involving an iPhone 5C used by one of the deceased San Bernardino shooters, the FBI—via the All Writs Act[44]—sought to compel Apple to write and sign new code (a new operating system) that would disable two security features purposely engineered by Apple to protect data stored on a phone.[45] These features prevent "brute force" attempts to break a user-created passcode by "[c]yber-attackers intent on gaining unauthorized access to a device . . . if given enough chances to guess and the ability to test passwords rapidly by automated means."[46] Specifically, "Apple imposes escalating time delays after the entry of each invalid passcode" and a setting, "if activated," that "automatically deletes encrypted data after ten consecutive incorrect attempts to enter the passcode."[47]

While some have accused the FBI of trying to compel Apple to produce a backdoor for law enforcement,[48] using backdoor in a metaphorical sense not as a term of art, from a *technical* perspective it would be more accurate to say that the FBI is trying

---

[43] *Id.*; *see also* Government's Ex Parte Application For Order Compelling Apple, *supra* note 40, at 3–4.

[44] 28 U.S.C. §1651(a) (2012). ("The Supreme Court and all courts established by Act of Congress may issue all s necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.").

[45] *See* Government's Ex Parte Application for Order Compelling Apple, *supra* note 40, at 4–8.

[46] Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance [hereinafter Apple's Motion to Vacate Order] at 6, *In re* the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M (C.D. Cal. Feb. 25, 2016.).

[47] *Id.*

[48] Apple characterizes the new operating system that the government attempts to compel it to create as "effectively a 'back door'" *Id.* at 2. Security Researcher Jeffrey I. Schiller has also suggested that "[i]n some ways, Apple's Signing key is a backdoor, in that it can be used to subvert the security of the iPhone. At this point Apple probably understands this as well. Fortunately, there are ways to close this particular backdoor. One simple way is to require that a phone be unlocked in order to install a software update." *See* Jeffrey I. Schiller, *It's About Security, not Privacy*, https://jis.qyv.name/home/pages/20160226 (last visited May 1, 2016).

to compel Apple to write code that exploits an existing vulnerability in the Apple iPhone 5C.[49] That is, iPhones will run code that Apple has signed, regardless of whether that code is "good code" that protects the security of the system, or "bad code" that intentionally weakens the security of the system.[50] The dangers of compelling the construction in communications networks of actual technical backdoors, which Professors Matt Blaze, Steve Bellovin, and others warn us all about, should not be conflated with what the FBI has attempted to compel Apple to do in the San Bernardino case. As the public and policy makers attempt to grapple with these very difficult and complex issues, such lexical confusion risks undermining the strong, powerful security arguments made against any compelled backdoor access. There should be an equally strong preference, therefore, for employing the term backdoor only in its precise technical sense when discussing the security of IP-based communications.

There are, however, legitimate security questions and concerns surrounding the FBI's demand in the San Bernardino case—but they should be framed accurately. While a full discussion of the particular security risks at issue is beyond the scope of this Article, two important policy considerations should be considered. First, as the Federal Trade Commission ("FTC") issues guidance strongly encouraging companies to use encryption to protect sensitive consumer information, [51] we should question concurrent

---

[49] Interview with Dr. Christopher Soghoian (Mar. 28, 2016).

[50] *Id.*

[51] *See* FEDERAL TRADE COMMISSION, *Start with Security: A Guide for Business* (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business ("Use strong cryptography to secure confidential material during storage and transmission. The method will depend on the types of information your business collects, how you collect it, and how you process it."). Moreover, when a company promises strong encryption to its customers, the FTC expects delivery of strong encryption. *See* FEDERAL TRADE COMMISSION, *Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data* (Jan. 2016), https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled ("'Strong encryption is critical for companies dealing with sensitive health information,' said Jessica Rich,

governmental actions that undermine the encryption and security features companies would purposely build into their products according to that guidance. Indeed, it is a bit incoherent for one arm of the government to encourage companies to develop and deploy the most secure, state of the art practices to secure customer data while another attempts to compel a company to undermine these very same practices. What equities does our government really want to protect here, and how are they to be promoted through its policies?

Second, while the San Bernardino case was resolved because the FBI bought an exploit from third party professional hackers[52] that allowed them to access the data on the phone,[53] the FBI and DOJ's proposed use of the All Writs Act to attempt to compel Apple to write code and sign that undermines core security features built into the iPhone raises the question of what other kinds of actions a company could be compelled to do in order to assist with the execution of a court order.[54] While each new kind of compelled action would be a legal question for courts to consider, security experts are concerned about the kind of precedent such an

---

Director of the FTC's Bureau of Consumer Protection. 'If a company promises strong encryption, it should deliver it.'").

[52] *See* Ellen Nakashima & Adam Goldman, *No Links to Foreign Terrorists Found on San Bernardino iPhone So Far, Officials Say*, THE WASHINGTON POST (April 14, 2016), *available at* https://www.washingtonpost.com/world/national-security/no-links-to-foreign-terrorists-found-on-san-bernardino-iphone-so-far-officials-say/2016/04/14/f1aa52ce-0276-11e6-9203-7b8670959b88_story.html ("Last month, a third party — professional hackers who hunt software flaws to sell — demonstrated to the bureau a method for unlocking the Apple iPhone of Syed Rizwan Farook, one of the shooters in the attack that killed 14 people.").

[53] *See generally supra* note 40 and accompanying text.

[54] Apple raises this concern in its Motion to Vacate Order. *See* Apple's Motion to Vacate Order, *supra* note 46, at 4, when it suggests that "if Apple can be forced to write code in this case to bypass security features and create new accessibility, what is to stop the government from demanding that Apple write code to turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on location services to track the phone's user? Nothing."

expansive reading of the All Writs Act could set.[55] For example, could the DOJ obtain a court order compelling companies to sign and deliver surveillance software though existing automatic update mechanisms?[56] Technologist Dr. Christopher Soghoian raises a significant cybersecurity harm that could flow from such compelled action:

> If consumers fear that the software updates they receive from technology companies might secretly contain surveillance software from the FBI, many of them are likely to disable those automatic updates. And even if you aren't worried about the FBI spying on you, if enough other people are, you will still face increased threats from hackers, identity thieves and foreign governments.
>
> There are a lot of parallels between computer security and public health, and in many ways, software updates are like immunizations for our computers. Just as we want parents to get their children immunized, we want computers to receive regular software updates. Indeed, just as the decision by some parents to not vaccinate their children puts their entire community a at risk, so too the decision to turn off automatic updates not only impacts the individual, but other users and organizations, as those vulnerable, infected users' computers will be used by hackers to target others.[57]

To be clear, the prior technical discussion of backdoors and the broader security questions at issue in the San Bernardino case is summary in nature, relying on the analyses and opinions of respected researchers in the computer science and security community and policy makers at the FTC. Drawing on this expertise and the conclusion that backdoors created for "good guys" can and will also be exploited by "bad guys," this Article begins with the premise that mandating the creation of backdoors in our communications networks and mobile devices is not a viable option for solving issues related to law enforcement access to communications data in an IP-based communications

---

[55] *See* Christopher Soghoian, *The Technology at the Heart of the Apple-FBI Debate, Explained*, THE WASHINGTON POST (Feb. 29, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/02/29/the-technology-at-the-heart-of-the-apple-fbi-debate-explained.

[56] *See id.*

[57] *Id.*

environment.[58] Moreover, this Article operates from the premise that we need to question and understand the broader security implications of an expansive reading of the All Writs Act, whether in the San Bernardino case or any other case where the government is attempting to compel a company to take actions that undermine the security of its networks, services, and products.

This Article does not, however, discount the fact that law enforcement faces certain challenges in an environment where it may no longer be able either to obtain access to data stored on a cell phone[59] or to intercept plain text communications content though traditional methods—i.e. getting a warrant. Indeed, in some circumstances, law enforcement may never have access to relevant data, or at least not in time to assist with an investigation. For better or worse, due to the mandates of CALEA and earlier smartphone technical architectures that allowed companies to bypass a user's password and provide data to the police, law enforcement became accustomed to an environment where the technical capabilities for gaining access to information were generally in place and easily available.[60] But that environment is changing and, without some new kind of CALEA-like mandate,

---

[58] Consistent with opinions expressed by computer scientists cited in this Article, security researcher Bruce Schneier succinctly explains the technical realities and consequences of any "exceptional access" scheme, whether providing access to encrypted data or not:

> As technologists, we can't build an access system that only works for people of a certain citizenship, or with a particular morality, or only in the presence of a specified legal document. If the FBI can eavesdrop on your text messages or get at your computer's hard drive, so can other governments. So can criminals. So can terrorists. This is not theoretical; again and again, backdoor accesses built for one purpose have been surreptitiously used for another. Vodafone built backdoor access into Greece's cell phone network for the Greek government; it was used against the Greek government in 2004-2005. Google kept a database of backdoor accesses provided to the U.S. government under CALEA; the Chinese breached that database in 2009.

Bruce Schneier, *Security or Surveillance*, LAWFARE (Feb. 1, 2016 1:01 PM), https://www.lawfareblog.com/security-or-surveillance.

[59] *See* Statement of James Comey, *supra* note 19.

[60] *See infra* Part II.

which seems unlikely in the near future,[61] law enforcement will be forced to adapt in different ways. How it will and should adapt is a critical discussion that law enforcement, policy makers, and the public must have.

The rhetoric surrounding the "Going Dark" debate or the current "Crypto War" has often been more divisive than productive[62] and, for the most part, not directed at identifying and obtaining what law enforcement *actually needs*, rather than what it wants ideally, in the current technological environment.[63] Indeed,

---

[61] It is impossible to predict the future. As of the writing of this article, the Administration has indicated it is not proposing legislation to mandate law enforcement access to communications content. Two senators have released a discussion draft of a bill that would, however, mandate law enforcement access to communications content, even when communications are encrypted end-to-end. This discussion draft is receiving significant criticism from the security community. *See generally supra* note 25; *see also*, Steven Bellovin, *Problems with the Burr-Feinstein Bill* SMBlog - STEVE BELLOVIN'S BLOG, https://www.cs.columbia.edu/~smb/blog/control/ (last visited Apr. 25, 2016).

[62] FBI Director James Comey has, for example, claimed that Apple and Google allow people to place themselves beyond the law:

> The notion that we would market devices that would allow someone to place themselves beyond the law, troubles me a lot. As a country, I don't know why we would want to put people beyond the law. That is, sell cars with trunks that couldn't ever be opened by law enforcement with a court order, or sell an apartment that could never be entered even by law enforcement. Would you want to live in that neighborhood? This is a similar concern. The notion that people have devices, again, that with court orders, based on a showing of probable cause in a case involving kidnapping or child exploitation or terrorism, we could never open that phone? My sense is that we've gone too far when we've gone there.

See Kashmir Hill, *FBI Director Says Apple and Google Are Putting Their Customers 'Beyond the Law'* FORBES (Oct. 13, 2014, 9:17 AM), http://www.forbes.com/sites/kashmirhill/2014/10/13/fbi-director-says-apple-and-google-are-putting-their-customers-beyond-the-law/#589474aa81cf.

[63] A report, *Don't Panic: Making Progress on the "Going Dark" Debate*, THE BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (2016) [hereinafter *Don't Panic*], is a noted exception to this statement. Another important exception is Steve Bellovin, Matt Blaze, Sandy Clark and Susan Landau's companion articles, *Going Bright: Wiretapping without Weakening Communications Infrastructure*, 14 IEEE SECURITY & PRIVACY 62 (2013) and

some of the rhetoric used by government officials in the current "Crypto War" has, at times, framed the debate primarily as a privacy issue, at best minimizing, at worst obfuscating the serious cybersecurity risks at stake.[64] A more constructive dialogue should

---

Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet, 12 NW. J. TECH. & INTELL. PROP. 1 (2014).

[64] *See* Devlin Bartlett, "*FBI Chief: Pendulum on Privacy 'Has Swung too Far*," THE WALL STREET JOURNAL (Oct. 16, 2014) http://blogs.wsj.com/law/2014/10/16/fbi-chief-pendulum-on-privacy-has-swung-too-far/ ("The head of the Federal Bureau of Investigation urged Silicon Valley Thursday to reverse course on encrypting phone data, suggesting the pendulum on privacy issues 'has swung too far' against the government in the wake of revelations by former National Security Agency contractor Edward Snowden.") *Id.* More recently, statements about the dispute between the FBI and Apple over access to encrypted data stored on the San Bernardino shooter's iPhone by FBI Director Comey and Apple CEO Tim Cook illustrate their different perspectives on the role encryption plays in society and its affect on public safety and security and the rule of law:

> FBI Director James Comey put this new predicament starkly in a congressional hearing on the San Bernardino case in February. "Law enforcement, which I'm part of, really does save people's lives, rescue kids, rescue neighborhoods from terrorists," he said. "And we do that a whole lot through court orders that are search warrants. And we do it a whole lot through search warrants of mobile devices. So we're gonna move to a world where that is not possible anymore? The world will not end, but it will be a different world than where we are today and where we were in 2014."
>
> Comey, who declined to be interviewed on this subject, has framed the conflict as a choice between privacy and security, a zero-sum trade-off. If it were that simple, Apple would have a steep battle indeed: whatever benefits we get from encryption would have to be weighed against the possibility of lives lost to acts of terrorism. But Cook flatly rejects this view as a red herring. "I think it's very simplistic and incorrect," he says. "Because the reality is, let's say you just pulled encryption. Let's you and I ban it tomorrow. And so we sit in Congress and we say, Thou shalt not have encryption. What happens then? Well, I would argue that the bad guys will use encryption from non-American companies, because they're pretty smart, and Apple doesn't own encryption.

Lev Grossman, *Inside Apple CEO Tim Cook's Fight With the FBI*, Time (Mar. 17, 2016) http://time.com/4262480/tim-cook-apple-fbi-2/.

recognize the *competing visions of security* at issue—that is, when strong cybersecurity practices and the critical equities they help to protect[65] may be at odds with certain aspects of law enforcement's traditional public safety mission.[66] Understanding and responding to the *full scope* and nature of law enforcement's challenges in the current technological environment is a complex inquiry and analysis that is beyond the scope of this Article. Moreover, any such comprehensive, nuanced analysis will require more information, gathered over time, from law enforcement investigations.

This Article attempts, however, to assist in focusing this analysis by examining how the ever-expanding Internet of Things ("IoT")[67] could give law enforcement at least some of what it needs, both with respect to increasing the availability of revelatory metadata and providing new, less problematic apertures for the

---

[65] "Each terrorist attack grabs headlines but the insidious theft of U.S intellectual property – software business plans, designs for airplanes automobiles pharmaceuticals etc. – by other nations does not. The latter is the real national-security threat and a strong reason for national policy to favor ubiquitous use of encryption." Susan Landau, The National Security Needs for Ubiquitous Encryption, Appendix A, *Don't Panic*, *supra* note 63.

[66] *See* Grossman, *supra* note 64; *see also*, Bruce Schneier, Security or Surveillance, Appendix A, *Don't Panic*, *supra* note 63 ("As framed in the media encryption debates are about whether law enforcement should have access to data or whether companies should be allowed to provide strong encryption to their customers. It's a myopic framing that focuses only on one threat – criminals including domestic terrorists – and the demands of law enforcement and national intelligence. This obscures the most important aspects of the encryption issue the security it provides against a much wider variety of threats. Encryption secures our data and communications against eavesdroppers like criminals, foreign governments, and terrorists. We use it every day to hide our cell phone conversations from eavesdroppers and to hide our Internet purchasing from credit card thieves Dissidents in China and many other countries use it to avoid arrest. It's a vital tool for journalists to communicate with their sources for NGOs to protect their work in repressive countries and for attorneys to communicate with their clients.") *Id*.

[67] The IoT, as used in this article, "refers to the ability of everyday objects to connect to the Internet and to send and receive data" Federal Trade Commission, Internet of Things: Privacy & Security in a Connected World, (Jan. 2015), FTC IoT Staff Report at i, [hereinafter *FTC IoT Staff Report*].

interception of communications content. Part of the method of examination will be a re-envisioning of what certain aspects of the 1999 IRA investigation described at the beginning of this Article might look like when recontextualized in 2016. Taking this investigation forward in time imaginatively will allow for a discussion of how capabilities in the current technological environment might aid or hamper that investigation and prosecution, giving some perspective on: (1) the types of investigative capabilities law enforcement gains and loses in a metadata-rich, post-CALEA, cybersecurity-centric encryption environment; (2) how such gains and losses can affect an investigation; and (3) how, notwithstanding the revelatory nature of some kinds of metadata and metadata analysis, metadata cannot always be a substitute for communications content in an investigation and prosecution.

Taking the IRA case forward in time will not illustrate every kind of investigative challenge facing law enforcement in the current technological environment. Rather, it is a vehicle to facilitate a productive dialogue about what law enforcement *actually needs* in a post-CALEA, cybersecurity-centric encryption environment. This discussion will, however, ultimately lead to some of the same privacy-focused debates about the appropriate scope of metadata collection and appropriate standards governing law enforcement access to metadata. It will also raise privacy questions about law enforcement use of IoT apertures to hear and see activities going on inside the home.

Part II of this Article examines the "Going Dark" and current "Crypto War" debate as, at least in part, a resource issue, which, in turn, illustrates the need for a concerted focus on determining what law enforcement actually needs in a post-CALEA, cybersecurity-centric encryption environment. Part III describes aspects of the IoT for purposes of understanding how it could aid law enforcement investigations. Part IV then examines how the IRA investigation described at the beginning of this Article might unfold in the current technological environment, with a particular focus on the IoT. Part V provides a brief conclusion.

II. THE CURRENT "CRYPTO WAR" AND "GOING DARK" DEBATE

Part II examines one key issue affecting the "Going Dark" debate—a resource issue that was identified even before many Silicon Valley firms started to encrypt user data by default. This discussion not only leads to a critique of the "Going Dark" metaphor itself, but also suggests the need for a focused dialogue to determine what law enforcement actually needs in a post-CALEA, cybersecurity-centric encryption environment. Accordingly, this Part ends by raising questions about how to evaluate what law enforcement needs in the current technological environment.

In early 2011, approximately three years before Apple kicked off the latest battle in the Crypto Wars with its expansion of encryption on iOS, then FBI General Counsel Valerie Caproni testified at a House Judiciary Committee hearing entitled *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*.[68] Using the "Going Dark" metaphor, she explained the interception challenges facing law enforcement in a technological environment devoid of the wiretapping capabilities envisioned by CALEA:

> In the ever-changing world of modern communications technologies . . . the FBI and other government agencies are facing a potentially widening gap between our legal *authority* to intercept electronic communications pursuant to court order and our practical *ability* to actually intercept those communications . . . . We call this capabilities gap the "Going Dark" problem. As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage—evidence that a court has authorized the government to collect. This gap poses a growing threat to public safety . . . . [D]ue to

---

[68] *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 2 (2011) [hereinafter *Going Dark Hearing*] (statement of Valerie Caproni, General Counsel, Federal Bureau of Investigation), https://judiciary.house.gov/wp-content/uploads/2011/02/Caproni02172011.pdf.

> the revolutionary expansion of communications technology in recent years, the government finds that it is rapidly losing ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA. This gap poses a growing threat to public safety . . . . [D]ue to the revolutionary expansion of communications technology in recent years, the government finds that it is rapidly losing ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA.[69]

Notably, this segment from Caproni's 2011 written statement does not address wiretapping problems due to encryption, but rather, the loss of capabilities due to consumer use of new IP-based communication services that are not covered by CALEA's wiretapping mandate. In her oral testimony, Caproni does, however, describe an environment where law enforcement wiretapping capabilities could be unduly hampered by encryption, requiring labor intensive, *individualized solutions* that could overwhelm law enforcement resources:

> There will always be criminals, terrorists, and spies who use very sophisticated means of communications that are going to create very specific problems for law enforcement. We understand that there are times when you need to design an individual solution for an individual target . . . . We are looking for a better solution for most of our targets, and the reality is, I think, sometimes we want to think that criminals are a lot smarter than they really are. Criminals tend to be some-what lazy, and a lot of times, they will resort to what is easy. And, so long as we have a solution that will get us the bulk of our targets, the bulk of criminals, the bulk of terrorists, the bulk of spies, we will be ahead of the game. We can't have individual—have to design individualized solutions as though they were a very sophisticated target who was self-encrypting and putting a very difficult encryption algorithm on for every target we confront because not every target is using such sophisticated communications.[70]

A year before Caproni testified, Google turned on HTTPS for Gmail, kick-starting a growing trend by tech companies enabling transport encryption by default.[71] A year later, Apple upped the

---

[69] *Id.* at 1.

[70] *Id.* at 52.

[71] *See* Ryan Singel, *Google Turns on Gmail Encryption to Protect Wi-Fi Users*, WIRED (Jan. 13, 2010, 2:25 PM), http://www.wired.com/2010/01/google-

ante by deploying end-to-end encryption in iMessage and FaceTime apps, thereby preventing the company from decrypting the communications content because it does not have access to the keys.[72] Apple also took steps to secure data stored on its mobile products by enabling disk encryption by default in its iOS operating system. Initially, this process used a key that was accessible to the company but, since 2014, the key encrypting data must be derived from the user's password, rendering these data inaccessible to the firm.[73] More specifically, while earlier versions

---

turns-on-gmail-encryption-to-protect-wi-fi-users/ (Gmail users will now default to HTTPS as communications travel between Google's servers and a user's computer. Google's prior default was to use HTTPS only for log-in, not for entire email sessions. While this switch does not encrypt the email, it prevents simple sniffing by hackers over insecure Wi-Fi connections). *Id*. While Google's use of HTTPS is arguably the start of a trend, the use of HTTPS does not significantly frustrate law enforcement surveillance because emails sent by Gmail users, at least for now, remain unencrypted while they sit stationary on Google's servers. Google has access to the stored email messages and generally can provide them to law enforcement when served with a warrant. More specifically, because Gmail's website uses HTTPS encryption, data sent between Gmail users and Google is encrypted as it travels between the user and Google's servers. As such, that data cannot be intercepted by law enforcement in "real time" with the assistance of a wiretap order served on a broadband ISP or telecommunications carrier. Law enforcement can, however, access the stored communications by compelling to Google to produce them with a court order.

[72] *See* John Evering, *Push for a More Secure Digital Privacy Irreversible After Edward Snowden Leaks*, THE NATIONAL (Feb. 11, 2015) http://www.thenational.ae/business/technology/push-for-a-more-secure-digital-privacy-irreversible-after-edward-snowden-leaks. For an explanation of end-to-end encryption, *see supra* note 25. With respect to iMessage text messages, however, such messages are backed up by default, *without encryption*, to Apple's iCloud service. Accordingly, unless the user disables the backup function, the text messages remain available to law enforcement with the appropriate court order, generally a warrant. *See, e.g.*, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[73] *See generally supra* notes 40–50 and accompanying text. *See also* Matthew Green, *Why Can't Apple Decrypt Your iPhone*, CRYPTOGRAPHYENGINEERING.COM (Oct. 4, 2014), http://blog.cryptographyengineering.com/2014/10/why-cant-apple-decrypt-your-iphone.html. Green notes:

> What's happened in the latest update is that Apple has decided to protect *much more of the interesting data on the device* under the

of iOS used encryption with a key *not known* to Apple for *some* data, iOS 8 expanded the use of this encryption to more kinds of user data—such as photos and text messages—that are generally of interest to law enforcement.[74] Google has also stated that it intends to encrypt its Android operating system by default, but the firm and its hardware partners have encountered technical issues resulting in most Android phones still remaining unencrypted.[75] More recently WhatsApp, a popular messaging service owned by Facebook and used by a billion people, now uses end-to-end encryption by default, and other firms such as SnapChat and Google are reported to be working on similar enhancements to their own services.[76]

> user's passcode. This includes photos and text messages -- things that were not previously passcode-protected, and which police very much want access to . . . . Previous versions of iOS also encrypted these records, but the encryption key was not derived from the user's passcode. This meant that (provided one could bypass the actual passcode entry phase, something Apple probably *does* have the ability to do via a custom boot image), the device could decrypt this data without any need to crack a password.

Id.

[74] *Id.*

[75] *See* Andrew Cunningham, *Android 6.0 Re-implements Mandatory Storage Encryption for New Devices*, ARSTECHNICA (Oct. 19, 2015, 3:53 PM), http://arstechnica.com/gadgets/2015/10/android-6-0-re-implements-mandatory-device-encryption-for-new-devices; interview with Dr. Christopher Soghoian (April 14, 2016).

[76] *See* Danny Yadron, *Facebook, Google and WhatsApp Plan to Increase Encryption of User Data*, THE GUARDIAN (Mar. 14, 2016, 6:00 PM), http://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increase-encryption-fbi-apple; *see also* Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED (Apr. 5, 2016), http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/ ("[T]oday, the enigmatic founders of WhatsApp, Brian Acton and Jan Koum, together with a high-minded coder and cryptographer who goes by the pseudonym Moxie Marlinspike, revealed that the company has added end-to-end encryption to every form of communication on its service. This means that if any group of people uses the latest version of WhatsApp—whether that group spans two people or ten—the service will encrypt all messages, phone calls, photos, and videos moving among them. And that's true on any phone that runs the app, from iPhones to Android phones to

For law enforcement, encryption that is enabled by default that also places keys solely in the hands of device holders significantly disrupts traditional forms of surveillance that have relied on third parties' (telecommunications providers and ISPs) having access to communications content, at least in most circumstances. As Caproni alludes to in her 2011 congressional testimony, without such third party access, law enforcement must find individualized investigative solutions.[77] In other words, time, energy, and resources must be expended to determine how to acquire data about a specific target that would otherwise readily be available from third parties with an appropriate court order without all these additional transaction costs. Caproni explains that, while law enforcement efforts can accommodate some of these individualized investigative necessities, an environment where encryption by default was the rule rather than the exception poses a potential financial and human resource burden that threatens significant harm to law enforcement's ability to pursue and fulfill its public safety mission.[78]

While it is certainly fair to recognize the changing investigative environment for law enforcement and the burden it places on law enforcement resources, the Berkman Center Report questions the very accuracy of the "Going Dark" metaphor itself.[79] The authors assert that "[s]hort of a form of government intervention in technology that appears contemplated by no one outside of the most despotic regimes, communication channels resistant to surveillance will always exist."[80] The Berkman Report broadly concludes that "communications in the future will neither be

---

Windows phones to old school Nokia flip phones. With end-to-end encryption in place, not even WhatsApp's employees can read the data that's sent across its network. In other words, WhatsApp has no way of complying with a court order demanding access to the content of any message, phone call, photo, or video traveling through its service. Like Apple, WhatsApp is, in practice, stonewalling the federal government, but it's doing so on a larger front—one that spans roughly a billion devices."). *Id.*

[77] *See supra* notes 68–69 and accompanying text.

[78] *See supra* notes 68–69 and accompanying text.

[79] *See Don't Panic*, *supra* note 63, at 9–15.

[80] *See id.* at 2.

eclipsed into darkness nor illuminated without shadow."[81] The report then offers several findings to support the thesis that, despite the recent developments in the employment of encryption by default in consumer communication products," law enforcement is not "Going Dark."[82] Two of these findings have particular import on how the IoT, as part of the current technological environment, gives law enforcement at least *some of what it needs*. Specifically, the IoT and its ever-expanding networked sensors may provide platforms and apertures for viewing activities and recording communications content.[83] Moreover, the IoT adds to the metadata-rich investigative environment available to law enforcement. Because most metadata is difficult to encrypt and is likely to remain unencrypted for the foreseeable future, it will continue to enhance law enforcement capabilities.[84]

These two observations about the IoT raise broader questions about how metadata and communications content function in investigations—that is: (1) how they aid investigations and prosecutions; (2) what different purposes they may serve; and (3) to what extent the ever-expanding availability and law enforcement access to metadata can counterbalance the loss of CALEA-like mandates for wiretapping capabilities for interception of communications content. Viewing the IoT as an ever-expanding array of potential apertures to aid surveillance also requires an examination of the extent to which such surveillance portals counterbalance some of the challenges posed to law enforcement by increasing encryption of communications content.

To be clear, these are not easy questions to answer because, to date, we have not been framing the underlying inquiry correctly. The Manhattan DA, for example, cites the fact that, between September 17, 2014 and October 1, 2015, his office was unable to execute 111 searches of smartphones running iOS 8.[85] As one

---

[81] *See id.* at 2.
[82] *See id.* at 8.
[83] *See id.* at 12–15
[84] *See id.* at 6.
[85] Manhattan DA report, *supra* note 20, at 9.

commenter observes, this example illustrates "the paradox at the heart of this debate: Because the data in question is encrypted, we will never know what information has been lost to analysts and investigators."[86] What we do not know is how many of these "failed search" cases, nevertheless, resulted in successful prosecutions. In other words, how often was encryption the dispositive issue? If such cases were prosecuted successfully, those prosecutions would inform the discussion about how encryption by default on smartphones was *actually* affecting law enforcement investigations. Rather than discussing such information, the DA's report focuses on the assumption that the "out of reach" data "would have been relevant to the case[s] [at issue] and to the investigation of additional crimes or perpetrators."[87] In order to better understand what law enforcement needs in the context of a current and changing technological environment that must accommodate *competing visions of security*, "we should stop looking for 'evidence' showing that terrorists and criminals use encryption and should instead look at the evidence that is available to analysts and investigators."[88] Only when we begin the complex task of assessing and analyzing the available information, or the information that *could be* available to law enforcement without a backdoor mandate, can we begin to understand how further to enable law enforcement investigations.

III. THE IOT

General Michael Hayden, former director of both the CIA and NSA, has made strong public statements against mandating backdoors.[89] Like many of the security researchers quoted in this

---

[86] Marshall Erwin, *The High Standard of Proof in the Encryption Debate,* JUST SECURITY (Feb. 5, 2016, 9:35 AM), https://www.justsecurity.org/29177/high-standard-proof-encryption-debate/.

[87] Manhattan DA Report, *supra* note 20, at 9.

[88] *See* Erwin, *supra* note 86.

[89] Lorenzo Franceschi-Bicchierai, *Former NSA Chief: I 'Would Not Support' Encryption Backdoors,* VICE MOTHERBOARD, (Oct. 6, 2015, 2:38PM), *available at* http://motherboard.vice.com/read/former-nsa-chief-strongly-disagrees-with-current-nsa-chief-on-encryption.

Article, General Hayden believes the security of the United States is "better served by stronger encryption, rather than baking in weaker encryption."[90] But Hayden warns civil libertarians not to rush to "get his autograph" because, as a former high-level official in the Intelligence world, he would forego backdoors in favor of "bulk data and metadata [collection.]"[91] While General Hayden's intelligence-based perspective[92] provides an important foil to the FBI Director's perspective and illustrates what is perhaps a significant tension between law enforcement and intelligence community perspectives in the context of the "Going Dark" debate,[93] he is certainly not the first to recognize the revelatory nature of metadata. Justice Sotomayor, for example, observes in her *United States v. Jones*[94] concurrence that aggregated location data:

> [G]enerates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, e.g., People v. Weaver, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour

---

[90] *Id.*

[91] Patrick Howell O'Neill, *Former NSA Chief Says U.S. Can Get Around Encryption with Metadata, Argues Against Backdoors*, THE DAILY DOT, (Jan 5, 2016, 10:42 AM), http://www.dailydot.com/politics/michael-hayden-encryption-debate-clinton-bush. General Hayden has, for example, argued for the necessity of the bulk collection of American's domestic calling records under a program previously authorized by the Foreign Intelligence Court under Section 215 of the USA Patriot Act. *See* Hayden-Soghoian Debate: Privacy vs. Intelligence Collection available at https://www.youtube.com/watch?v=6aRklrv3r34.

[92] To be fair, General Hayden acknowledges that in the context of the "Going Dark" debate, "[e]ncryption is 'a law enforcement issue more than an intelligence issue' [because,]" Hayden argued "frankly intelligence gets to break all sorts of rules to cheat to use other paths." *Id.*

[93] *See* Carrie Cordero, LAWFARE, *Is There a National Security-Law Enforcement Divide on "Going Dark"?*, Lawfare (Feb. 3, 2016, 7:00 AM) *available at* https://lawfareblog.com/there-national-security-law-enforcement-divide-going-dark.

[94] United States v. Jones, 132 S.Ct. 945, (2012).

> motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. Pineda-Moreno, 617 F. 3d, at 1124 (opinion of Kozinski, C. J.).[95]

The IoT—which "refers to the ability of everyday objects to connect to the Internet and to send and receive data"[96]—promises to augment immeasurably a communications environment already teeming with metadata that reveals "personal information, habits, locations and physical conditions over time."[97] Indeed, as the FTC notes in a January 2015 Staff Report, "experts estimate that, as of [2015], there will be 25 billion connected devices, and by 2020, 50 billion."[98] The kinds of IoT devices now available to consumers are already too numerous to list here—and new ones come on the market every day—but illustrative examples include smart thermostats, automation systems for home lights and appliances, and bracelets that track your physical activity.[99] Such products are proliferating to the degree that the Berkman Center Report projects that the IoT "has the potential fundamentally to shift the way we interact with our surroundings[:]"[100]

> Appliances and products ranging from televisions and toasters to bed sheets, light bulbs, cameras, toothbrushes, door locks, cars, watches and other wearables are being packed with sensors and wireless connectivity. Numerous companies are developing platforms and products in these areas. To name but a few, Phillips, GE, Amazon, Apple, Google, Microsoft, Tesla, Samsung, and Nike are all working on products with embedded IoT functionality, with sensors ranging from gyroscopes, accelerometers, magnetometers, proximity sensors, microphones, speakers, barometers, infrared sensors, fingerprint readers, and radio frequency antennae with the purpose of sensing, collecting, storing, and analyzing fine grained information about their surrounding environments. These devices will all be connected to each other via the Internet, transmitting telemetry data to their respective vendors in the cloud for processing.[101]

---

[95] *Id.* at 955.
[96] *FTC IoT Staff Report*, *supra* note 67.
[97] *Id.* at ii.
[98] *Id.* at i.
[99] *Id.*
[100] *Don't Panic*, *supra* note 63, at 13.
[101] *Id.*

One researcher, Charles Givre, explored and tested the kinds of information that can be learned about an individual through the IoT networked devices she uses.[102] Specifically, Givre presented the results of an experiment designed to document the wealth of information collected and stored through everyday use.[103] An abstract of his presentation notes that Givre "approached [the] experiment like a law enforcement or intelligence investigation, beginning with a bit of seed knowledge about the target, and built a profile about the target using the data that was available via these devices' APIs[104] and the data they transmit over the Internet."[105] The IoT devices at issue in Givre's investigation include a Wink Hub (a platform that allows control of Internet-connected home devices from a single screen), a Nest Thermostat, and an Automatic car dongle.[106] Examination of even a small segment of Givre's investigation suggests the broad scope of data potentially available to law enforcement through *following the IoT*. The investigation begins with Givre focusing only with the knowledge that the "target" (the target in this case is Givre) owned a Wink Hub.[107] From this point, Givre was able to determine the target's

---

[102] Lauren Kirchner, *Your Smart Home Knows A Lot About You,* PROPUBLICA, (Oct. 9, 2015, 1:00 PM), https://www.propublica.org/article/your-smart-home-knows-a-lot-about-you?google_editors_picks=true.

[103] *Id.*

[104] "In the simplest terms APIs are sets of requirements that govern how one application can talk to another. APIs aren't at all new whenever you use a desktop or laptop APIs are what make it possible to move information between programs, for instance by cutting and pasting a snippet of a LibreOffice document into an Excel spreadsheet. System-level APIs makes it possible for applications like LibreOffice to run on top of an OS like Windows in the first place." Brian Proffitt, *What API's Are And Why They're Important,* READWRITE, (Sept. 19, 2013), http://readwrite.com/2013/09/19/api-defined.

[105] Charles Givre, Booze Allen Hamilton, *What Does Your Smart Device Know About You?* STRATA + HARDOOP (Sept. 30, 2015), http://conferences.oreilly.com/strata/big-data-conference-ny-2015/public/schedule/detail/42710.

[106] *Charles S. Givre, Booz Allen Hamilton, Presentation at Strata NYC 2015, What Does Your Smart Device Know About You?*, *available at* http://cdn.oreillystatic.com/en/assets/1/event/132/What%20does%20your%20smart%20device%20know%20about%20you_%20%20%20Presentation.pdf.

[107] *Id.* at slide 5.

Facebook ID and Twitter handle, and to identify the other devices owned or controlled by the target, which included a Nest Thermostat.[108] From the Nest Thermostat, Givre learned that the target uses Comcast for Internet service, that the target lives in Pikesville, Maryland and owns both an iPhone and iPad.[109]

Although access to the data produced by these devices is typically protected by an email address and password,[110] Givre notes that the devices store data on remote cloud servers, rather than locally.[111] Remote cloud storage often gives law enforcement the ability to obtain data, since it is held by and accessible to a third party provider to whom law enforcement need only present an appropriate court order. While there may be no mandates to require retention of the data, having access to it is often part of a company's revenue stream and product functionality.[112] If Givre's investigation were an actual one performed by law enforcement, the identification of these various accounts could provide a range of information about the target, including his interests and associates (via Twitter) and his likely comings and goings from the home (via Nest).[113]

Again, this discussion only highlights a small selection of IoT networked devices that may operate in a target's life and references only some of the kinds of data they could provide to law enforcement. What is particularly important about Givre's work for law enforcement (and what may already be part of law enforcement investigative practices) is his illustration of how it is

---

[108] *Id.* at slide 22.
[109] *Id.* at slide 41.
[110] *Id.*at slide 9.
[111] *Id.* at slide 7.
[112] Consider, for example, that the iCloud backup service is enabled by default on Apple devices (the automatic backup can, of course, be disabled by users). Although Apple encrypts iCloud backup services, it holds the keys. Law enforcement can, therefore, compel Apple to turn over data stored in the iCloud with the appropriate court order, generally a warrant. The Berkman Center Report also notes that "the majority of businesses that provide communication services rely on access to user data for revenue streams and product functionality should a password be forgotten." *Don't Panic*, *supra* note 63, at 3.
[113] Givre, *supra* note 105, at slides 43–48.

possible to start with a single bit of information about a networked device used by a target, then build a profile about the target's broader use of networked devices, which can lead to relevant information for an investigation. Following this meticulous investigative path—*following the IoT*—enables law enforcement to design *individualized* investigative plans for targets based on the kinds of devices they use and the kinds of metadata or public source content (think Twitter and Facebook)[114] such devices and services reveal.

It should also be noted that Givre performed his investigation without any "privileged access"—that is, without the ability to compel information from ISPs in order to determine what devices are present in the home and calling back to the manufacturer. Law enforcement could, however, compel such information from, for example, Comcast or Verizon.[115]

In addition to the public source content that may be revealed through *following the IoT*, the IoT provides a range of apertures that may allow law enforcement to record private conversations or view activities occurring in private spaces. These surveillance "opportunities" can generally be categorized in two different ways, the first of which is company assistance. As noted in the Berkman Center Report, "[t]he audio and video sensors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications."[116] In other words, law enforcement may be able to compel assistance from companies whose products are capable of recording conversations or activity, "whether through one's own smartphone, an Amazon Echo, a baby monitor, an Internet-enabled security camera, or a futuristic 'Elf on a Shelf' laden with networked audio and image sensors."[117]

---

[114] Of course, law enforcement may not need IoT information to find a target's public Twitter or Facebook account.

[115] *See* Stored Wire and Electronic Communications and Transactional Records Access (SCA),18 U.S.C. §§ 2701–2712 (2010); Pen Registers and Trap and Trace Devices (Pen/Trap), 18 U.S.C. §§ 3121–3127 (2010).

[116] *Don't Panic*, *supra* note 63, at 13.

[117] *Id.* at 13–14.

As noted in the Berkman Center Report, there is some legal support for this kind of compelled company assistance. Specifically, in *The Company v. United States*,[118] the FBI, under Wiretap Act authority for "bugging" individuals suspected of criminal activity, sought to compel the Company to use its on-board driver assistance technology to record conversations going on inside a car.[119] One feature of the technology allows the Company to open "a cellular connection to a vehicle and listen to oral communications within the car" as part of the stolen vehicle recovery mode.[120] When the system is in stolen recovery vehicle mode, however, passengers in the car cannot use any of the other "on board" system services—they are completely disabled.[121] If, for example, the customer presses an emergency button while the recovery mode is enabled, the customer will not be connected to the response center—only the FBI will be listening in on the line.[122] Ultimately, the court did not order the Company to assist the FBI because such compelled assistance violated the "minimum of interference" language of the Wiretap Act.[123] While the court found that the "minimum of interference" requirement allows for "some level of interference with customers' service in the conducting of surveillance," such "eavesdropping is not performed with 'a minimum of interference' if a service is *completely* shut down as a result of the surveillance."[124] While this case was not decided in the government's favor, other kinds of IoT company-compelled assistance may be upheld, as long as the surveillance

[118] The Company v. United States, 349 F.3d 1132 (9th Cir. 2003).
[119] *Id.* at 1133.
[120] *Id.* at 1133–34.
[121] *Id.* at 1134, 1145.
[122] *Id.* at 1135.
[123] *Id.* at 1145 ("Our interpretation of the minimum of interference language is bolstered by our reading of title III which we believe does not evince a congressional intent to authorize surveillance in the face of complete disruption of a wire and electronic communication service for a particular customer.").
[124] *The Company*, 349 F.3d at 1145 (emphasis in original).

would not completely disable the intended use of the product or service.[125]

Second, IoT networked devices can provide apertures for hacking (assuming such hacking is lawful),[126] where law enforcement would enable audio or video features of a networked device or use one device to obtain access to the target's network or user credentials, potentially facilitating the collection of information from a user's computer or other networked device. In recent written congressional testimony, the Director of National Intelligence, James Clapper, explained that:

> "Smart" devices incorporated into the electric grid, vehicles—including autonomous vehicles—and household appliances are improving efficiency, energy conservation, and convenience. However, security industry analysts have demonstrated that many of these new systems can threaten data privacy, data integrity, or continuity of services, in the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.[127]

Former CIA Director, David Petraeus, echoed this same message earlier in 2012, explaining that:

> Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters — all connected to the next-generation internet using abundant, low-cost, and high-power computing.[128]

---

[125] *Id.* ("We need not decide precisely how much interference is permitted. A minimum of at least precludes total incapacitation of a service while interception is in progress.").

[126] *See* Bellovin, Blaze, Clark, & Landau, *supra* note 63; *see also infra* note 130.

[127] *Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before the S. Select Comm. on Intelligence*, 114th Cong. 1 (2016) (statement of James R. Clapper, Director of National Intelligence), http://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing.

[128] Spencer Ackerman, *CIA Chief: We'll Spy on You Through Your Dishwasher*, WIRED, (Mar. 15, 2012, 5:35 PM) http://www.wired.com/2012/03/petraeus-tv-remote.

Moreover, a researcher looking at IoT security from a military perspective characterizes IoT as "a new attack surface."[129] While these are Intelligence Community and Military perspectives, some such capabilities are not *per se* outside the reach of all law enforcement, as long as they are appropriately authorized, resourced, and overseen.[130] Indeed, a group of distinguished

---

[129] KONRAD WRONA, SECURING THE INTERNET OF THINGS: A MILITARY PERSPECTIVE 503 (IEEE, 2015) Specifically, the attack surface consists of: "IoT devices (i.e. sensors and actuators)," "Communication channels between the devices as well as between the devices and the back-end system," "IoT-specific back-end applications," and "Back-end data storage." *Id.*

[130] *See* Bellovin, Blaze, Clark, & Landau, *supra* note 63. There are a number of law enforcement hacking activities (often referred to as Network Investigative Techniques) that are becoming public, with at least one dating back thirteen years. *See* Matt Apuzzo, *F.B.I. Used Hacking Software Decade Before iPhone Fight, New York Times* (April 13, 2016) http://mobile.nytimes.com/2016/04/14/technology/fbi-tried-to-defeat-encryption-10-years-ago-files-show.html?_r=2. In early 2003, FBI agents hit a roadblock in an investigation called Operation Trail Mix. *Id.* While agents had been intercepting phone calls and emails of their targets, encryption software suddenly made the emails unreadable. *Id.* The investigators, in what is believed to be first example of the FBI "remotely installing surveillance software, known as spyware or malware, as part of a criminal wiretap" convinced a judge to let them "remotely and secretly" install the malware on the targets' computers to help agents thwart the encryption. *Id.* "'This was the first time that the Department of Justice had ever approved such an intercept of this type,' an FBI agent wrote in a 2005 document summing up the case." *Id.*

Other, more recent examples of law enforcement hacking include: *In the Matter of the Search of Network Investigative Technique ("NIT") for Email Address texan.slayer@yahoo.com*, Third Amended Application For A Search Warrant (Case No. 12-sw-05685-KTM) (US Dist. Ct., D. of Colorado) (Dec. 11, 2012) ("[T]he NIT is designed to collect the items described in Attachment B – i.e., information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of Section 1038 of Title 18, United States Code (False information and hoaxes."). *Id.* at 16; *In Re Warrant to Search A Target Computer At Premises*, Memorandum and Order (Case. No. H-13-234M) (US Dist. Ct. Southern Dist. Of Texas, Houston Division) (April 22, 2013) ("The search would be accomplished by surreptitiously installing software designed not only to extract certain stored electronic records but also to generate user photographs and location information over a 30-day period. In other words, the

computer scientists have identified a need to develop a "lawful hacking" legal framework that could support law enforcement exploitation of existing vulnerabilities in software and mobile devices, which the authors maintain is a more secure alternative to the purposeful introduction of backdoors into our networks and mobile devices.[131]

Part IV will look at how the IRA case might be investigated in 2016, with a particular focus on capabilities and information that may be available from exploitation of networked IoT devices.

IV. BRINGING THE IRA INVESTIGATION FORWARD IN TIME: WHAT KIND OF CAPABILITIES AND INFORMATION WOULD BE AVAILABLE TO LAW ENFORCEMENT NOW?

Through a reasonable exercise of the imagination, it is possible to envision how the IRA investigation might proceed in 2016's technological environment. The purpose of this exercise is to illustrate at least some of the *current* investigative capabilities and information types available to analysts and investigators, in order to compare and contrast them with the tools available during the actual investigation and thus begin to assess what law enforcement *actually needs* in a post-CALEA, cybersecurity-centric encryption era. This single case cannot offer a comprehensive analysis on the subject. Indeed, an ongoing, rigorous case-by-case analysis is needed with law enforcement providing: (1) information about failures to obtain evidence due to an inability to acquire IP-based communications data (in motion or stored on a mobile), which consequently prevented the pursuit of a successful investigation and prosecution; and (2) information about failures to obtain evidence due to an inability to acquire IP-based communications data (in motion or stored on a mobile device) that, nevertheless, result in a successful investigation and prosecution. In other words, we need continually to assess what is available, what is missing, and how the inability to access information in a timely fashion is

---

Government seeks a warrant to hack a computer suspected of criminal use. For various reasons explained below, the application is denied."). *Id.* at 1.

[131] Bellovin, Blaze, Clark, & Landau, *supra* note 63.

affecting law enforcement investigations. With this kind of information in hand, policy makers would be in a much better position to determine what kinds of new capabilities law enforcement actually needs and what new statutory authorities are necessary for law enforcement to employ those capabilities. Part of this analysis must include an examination of the differing functions metadata and content [132] may serve in an investigation and prosecution and the speed at which such information may or may not be available to law enforcement in the current technological environment.

The condensed narrative of the IRA investigation presented in the Introduction can, more or less, be outlined in the following way:

(1) An ongoing weapons smuggling operation was discovered. In addition to stopping the flow of weapons, law enforcement needed to determine both who was part of the operation and the intended use or purpose for the acquired weapons.[133]

(2) Answering these questions began with tracing the first gun back to a gun dealer in South Florida, which identified a female gun purchaser. [134] Express Mail information on the recovered packages led agents back to the particular post offices in South Florida where some of the mailings occurred, and video of the mailings and express mail records kept by the Post Offices helped agents identify two men who mailed packages.[135]

---

[132] For purposes of this discussion, content is being defined per the definition found in the Wiretap Act: "'contents', when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (2004). I have argued elsewhere that the content/non-content distinction as defined the in the Wiretap Act and the Pen/Trap statute is no longer a viable, workable distinction in an IP-based communications environment. *See* Steven M. Bellovin, Matt Blaze, Susan Landau, & Stephanie K. Pell, *It's Too Complicated: The Technological Implications of IP-based Communications on Content/ Non-Content Distinctions and the Third Party Doctrine*, (forthcoming) HARV. J. L. & TECH. (2016).

[133] *See* United States v. Claxton, *supra* note 1.

[134] *Id.*

[135] *Id.*

(3) Physical surveillance of these identified suspects led to the identification of an additional male suspect.[136] Through discovery of locations where more weapons were purchased, it was determined that the male suspect had also purchased some of the weapons.[137]

(4) While others associated with the original four suspects were identified in the course of the investigation, no one else was indicted, save one gun dealer who had falsified federal forms required to sell the weapons to the female and male gun purchasers.[138] Moreover, the means of identification of potential co-conspirators was limited mostly to physical surveillance and the examination of various kinds of records associated with the gun purchases, the mailing of the packages, and financial accounts where deposits were made to fund the gun smuggling operation.[139]

(5) While investigators had suspicions that the gun running operation might be tied to IRA activities,[140] the *purpose* of the operation and the defendants' intentions for the weapons were not known until the defendants were arrested and the lead defendant told agents that this was an IRA operation and that the weapons were meant to kill British police and Protestant paramilitary forces.[141] The lead defendant also indicated that the peace process had failed and the weapons were meant to replace the cache of weapons being publicly turned over as part of the Good Friday Agreements.[142] Various documents and other physical items retrieved in post-arrest searches of places where the defendants lived corroborated the statements made by the lead defendant.[143] These statements were necessary evidence for the purpose of

---

[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.* For example, the packages were en route to addresses in the Republic of Ireland and the return addresses on the packages came to non-existent places and all of the defendants, other than the gun dealer, were of Irish descent. *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*

proving the most serious charge lodged in the case, a conspiracy to murder or maim persons in a foreign country in violation of 18 U.S.C. § 956(a)(1). [144] Additional weapons, some that were packaged and ready to be mailed, were also discovered in the post-arrest searches of homes.[145]

By taking this case forward in time to the technological environment of 2016, which requires some reasonable speculation and imagination, it is possible to envision how metadata and content would assist investigators. Once the first weapon was discovered at Coventry Airport, the three critical challenges were: (1) finding and/or intercepting all additional weapons that were part of the operation; (2) identifying all of the individuals involved in the operation; and (3) determining the purpose of the operation. It would be fair to characterize the defendants as practicing relatively good operational security ("OPSEC") for 1999. While investigators discovered that some of the defendants had cell phones, the phones did not provide useful information during the course of the investigation—indeed, one subject evaded physical surveillance on the day of arrest and traveled north, only to be located later in Philadelphia.[146] Additional co-conspirators were not located through cell phone usage and, to our knowledge, the defendants did not communicate over the phone.[147] As far as we could tell, per actual physical surveillance, communication occurred during in person meetings at bars, gas stations, and inside of defendants' apartments.[148]

In 2016, however, it is a bit harder to "stay off the grid." The use of cell phone location data, whether through real-time tracking, historical records, cell-tower dumps, or community of interest requests,[149] which can reveal previously unknown associations by

---

[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] For a description of different ways that law enforcement uses cell phone location information to track suspects, *see* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law*

showing phones that "occupied" the same places at the same time,[150] are now available to law enforcement. Assuming the 2016 suspects[151] are carrying mobile devices, it arguably would be quicker and more efficient today to identify their associates and possible co-conspirators than it was in 1999. As previously noted, the IRA case was an ongoing operation when discovered, and only the four defendants were arrested and prosecuted for purchasing and shipping the weapons overseas.[152]

Let's assume, as was true in 1999, that the suspects do not communicate using unencrypted voice communication channels. More specifically, let's assume, according to current tradecraft, that when they do communicate using a smartphone, they use an App for sending end-to-end encrypted texts or making encrypted calls. The content of those communications is, therefore, not available to law enforcement through the traditional means either of serving a provider with a warrant for stored communications or a Title III Wiretap order for intercepting the communications in real-time. Law enforcement, however, needs to know the purpose of the smuggling operation, since it would assist in determining who may be in danger, as well as provide important evidence of intent, which goes towards proving that the suspects are conspiring to murder or maim individuals in a foreign country. The *metadata* from cell phones or other mobile or wearable devices is unlikely to reveal that kind of information. As previously referenced, it is more likely to assist in finding and tracking a suspect, learning about the patterns of his daily life and mapping out his web of associates.[153] In the actual IRA case, the *content* evidence necessary to reveal the purpose of the smuggling operation and that the defendants were part of a conspiracy to murder or maim

---

Enforcement Access to Location Data That Congress Could Enact, 27 BERKELEY TECH. L. J. 117, 119–33, 152–53 (2012).

[150] Pell & Soghoian, *supra* note 149, at 152–53.

[151] The term "suspect" is used when talking about a 2016 re-visioning of the IRA case and "defendant" is used when talking about the defendants in the actual IRA case in 1999–2000.

[152] *See* United States v. Claxton, *supra* note 1.

[153] *See* U.S. v. Jones, 132 S. Ct. at 955.

individuals in a foreign country did not come until after the defendants were arrested and the lead defendant gave a confession to the FBI case agent. As is often the case in an investigation, there are no guarantees of "forthcoming" evidence—you work an investigation and use the lawful resources available to you, some of which involve good interviewing skills.

Still, in today's environment, law enforcement is right to be concerned that communications content, which can be critical to the successful investigative and prosecutorial elements of a case, (including the ability to stop an attack before it happens), is becoming increasingly unavailable through the traditional means of compelling the information from a third party with the appropriate court order. One method to gain access to encrypted communications associated with smartphones is to hack the phones of targets, infecting them with malware capable of capturing voice communications and keystrokes before they are encrypted.[154] Moreover, the IoT is providing new kinds of apertures that could facilitate the sound and video recording of communications and activities occurring in private spaces, whether via company assistance or through hacking by the police. Determining what apertures may be available and exploitable based on the kind of IoT devices enabled in a home or office could, in some cases, be a time-intensive process. Accordingly, while communications may be accessible, such access may not be as readily available as in a CALEA-like framework. Given that the defendants were not talking on phones in the IRA case, it would have been worth considering how IoT devices could have been exploited in their apartments or the cars they drove, had such technology only been available in 1999. Of course, bugging a room is not a new technique, but it generally requires direct physical access to the room, often through surreptitious means. Direct physical access is risky, both in terms of physical risk to the agents and the risk of

[154] Interview with Dr. Christopher Soghoian (April 14, 2016); *see also* Bellovin, Blaze, Clark, & Landau, *supra* note 63; for a discussion of law enforcement hacking see *supra* note 130.

compromising the investigation,[155] which presumably limits the regularity[156] and efficacy of the technique.

With the IoT, however, such "bugging," whether to record sound or video, is not limited by physical access, nor is it necessarily burdened due to the risk of discovery or harm to the officers. Moreover, unlike the traditional wiretapping of phones, recording the sounds and sights going on inside the home has the potential to reveal a broader array of sensitive, personal information, some of which could also be highly relevant to an investigation.

In the IRA case, all defendants were convicted of a series of charges relating to the gun smuggling operation.[157] None, however, was convicted of the most serious charge of conspiring to murder or maim individuals in a foreign country—even though the lead defendant's post-arrest statements were admitted in the trial without any limiting instructions regarding their applicability to the other defendants.[158] Sometimes, no matter how strong the evidence is, juries do not convict.

V. CONCLUSION

The FBI Director and Manhattan DA raise legitimate concerns about how a post-CALEA, cybersecurity-centric encryption era will affect law enforcement's ability to carry out its traditional public safety mission. This Article takes the position that mandated backdoors are not a viable option for enabling law enforcement access to communications data because the attendant cybersecurity risks are too great. As policy makers grapple with these *competing*

---

[155] A law enforcement officer could be harmed or an operation thwarted if agents were caught trying to install a bug.

[156] In the most recent Wiretap Act Report, only three instances of wiretapping via "Oral, (Incl. Microphone, Eavesdrop)" were reported for the calendar year Jan. 1, 2014 through Dec. 31, 2014 in comparison to 2,270 instances of wiretapping via "Wire (Incl. Any Type of Telephone: Standard, Cell, Mobile)" *Wiretap Report 2014* (Dec. 31, 2014), at Table 6, http://www.uscourts.gov/statistics-reports/wiretap-report-2014.

[157] *See* United States v. Claxton, *supra* note 1.

[158] *Id.*

visions of security, they must determine what law enforcement *actually needs* in the current technological environment. The IoT will augment immeasurably the variety and amount of revelatory metadata, which can assist law enforcement in myriad ways, from locating and tracking a target, to identifying his associates and discerning the routines and patterns of activity in his life. With respect to communications content, the IoT offers new apertures for audio and video recording of communications and activities inside public spaces.

As policy makers consider what law enforcement *actually needs* and what, if any, changes to the law are required for law enforcement to execute certain functions effectively, the pubic discussion must also account for the privacy implications of, among other things, the smart-sensored home. An IoT-enabled home, office, or other private space offers law enforcement the ability to enter the home and record conversations and activities in ways that were not possible in the past, save for the relatively infrequent installation of a bugging device, which required physical access to the home. Perhaps a useful counterbalance to law enforcement's challenges in the current technological environment, the smart home is a potentially bountiful surveillance platform. Some yet uncreated avatar of the popular child's toy "Elf on the Shelf" [159] or its Jewish equivalent, the "Mensch on a Bench,"[160] may ultimately become a "Snoop on the Stoop" invited to sit in our homes with a seemingly benign doll's smile, sporting one of many new sets of IoT eyes and ears.

---

[159] *Don't Panic*, *supra* note 63, at 14. *See* THE ELF ON THE SHELF, http://elfontheshelf.com (last visited Apr. 17, 2016).

[160] *See* THE MENSCH ON A BENCH, http://themenschonabench.com (last visited Apr. 17, 2016).