William & Mary Bill of Rights Journal

Volume 26 | Issue 2 Article 8

Private Actors, Corporate Data and National Security: What Assistance Do Tech Companies Owe Law Enforcement?

Caren Morrison

PRIVATE ACTORS, CORPORATE DATA AND NATIONAL SECURITY: WHAT ASSISTANCE DO TECH COMPANIES OWE LAW ENFORCEMENT?

Caren Morrison*

ABSTRACT

When the government investigates a crime, do citizens have a duty to assist? This question was raised in the struggle between Apple and the FBI over whether the agency could compel Apple to defeat its own password protections on the iPhone of one of the San Bernardino shooters. That case was voluntarily dismissed as moot when the government found a way of accessing the data on the phone, but the issue remains unresolved.

Because of advances in technology, software providers and device makers have been able to develop almost impenetrable protection for their customers' information, effectively locking law enforcement out of accounts and devices, even when armed with a search warrant. Most privacy watchdogs, understandably shaken by Edward Snowden's revelations of NSA spying, argue that this is an unadulterated good. The prosecutorial view is that this is an unprecedented interference with lawful investigations.

There is no question that the companies fashioning themselves as champions of privacy benefit financially from this position. Apple has openly admitted in court filings that complying with court orders to assist in the execution of search warrants could "substantially tarnish Apple's brand." But while Apple may bear some responsibility for creating a system that it could not access itself, does that mean they should be statutorily tasked with undoing it?

Current statutory law, in particular the Communications Assistance for Law Enforcement Act (CALEA), does not cover the encrypted information on physical devices, or information companies' responsibilities to decrypt it. This Essay takes the question of whether CALEA should be amended as a starting point for a broader exploration of what assistance the government can justly ask of its citizens.

There are strong arguments to be made that such obligations would not be reasonable, or that there should be a zone of privacy that the government cannot

* Associate Professor of Law, Georgia State University College of Law. I am grateful to Russ Covey, Dan Richman, Nirej Sekhon, and especially Steve Morrison (no relation), without whom this Essay would not have materialized at all. Thanks to Adam Gershowitz, Jeff Bellin, and the editorial board of the *William & Mary Bill of Rights Journal* for putting on such a thought-provoking symposium.

access. This would support a system in which some warrants are ineffectual. But if the functional impossibility of execution of these warrants is just the byproduct of a corporate strategy, "them's the breaks" seems like an insufficient justification.

INTRODUCTION

When the government investigates a crime, do citizens have a duty to assist? This question was raised in the struggle between Apple and the FBI over whether the agency could compel Apple to defeat its own password protections on the iPhone of one of the San Bernardino shooters.[1] That case was voluntarily dismissed as moot when the government found a way of accessing the data on the phone.[2] However,

---

[1] *See* Devlin Barrett, *Apple Fight Gets Technical: Justice Department, Apple Trade Salvos Over Basic Issues in Locked-iPhone Case*, WALL ST. J., Feb. 22, 2016, at B1. Apple's recalcitrance was new; in the past, Apple had been able to easily assist law enforcement agencies in accessing password-protected iPhones. Joel Rose, *The Seeds of Apple's Standoff with DOJ May Have Been Sown in Brooklyn*, NPR (Feb. 22, 2016, 5:16 AM), http://www.npr.org/2016/02/22/467602161/the-seeds-of-apples-standoff-with-doj-may-have-been-sown-in-brooklyn [https://web.archive.org/web/20171113021316/https://www.npr.org/2016/02/22/467602161/the-seeds-of-apples-standoff-with-doj-may-have-been-sown-in-brooklyn]. This easy access, however, meant that malefactors might also bypass privacy protections. *See* Corinne Ramey, *DA Can't Unlock 423 Apple Devices*, WALL ST. J., Nov. 18, 2016, at A11A. Apple, therefore, developed a more advanced operating system that contained protocols that protected iPhone users from unwanted intrusions. Devlin Barrett et al., *Apple, Others Encrypt Phones, Fueling Government Standoff*, WALL ST. J., Nov. 19, 2014, at A1. By design, Apple ensured that it could not easily bypass the protections either. *See* Steven R. Morrison, *Breaking iPhones Under CALEA and the All Writs Act: Why the Government Was (Mostly) Right*, 38 CARDOZO L. REV. 2039, 2041 (2017).

[2] Morrison, *supra* note 1, at 2043–44.

the issue remains unresolved, even as the government has asked Apple to unlock other iPhones,[3] and Apple continues to refine its encryption technology.[4]

Because of advances in technology, software providers and device makers have been able to develop almost impenetrable protection for their customers' information, effectively locking law enforcement out of accounts and devices, even when armed with a search warrant.[5] Most privacy watchdogs, understandably shaken by Edward Snowden's revelations of NSA spying, argue that this is an unadulterated good.[6] The prosecutorial view is that this is an unprecedented interference with lawful investigations.[7]

In the early 1990s, when telephonic communications were moving from copper wire based technology to fiber optics, the government faced a similar challenge. Because of the change in interception technology, it could no longer conduct wiretaps and obtain pen registers without assistance from the telephone company.[8] The issue was resolved by the passage of the Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994.[9] CALEA placed an affirmative duty on "telecommunications carriers" to ensure that, regardless of how their technology evolved, they retained the ability to assist the government with lawful interceptions.[10]

The challenge of encryption and unbreakable smartphones has updated this issue for today. Until recently, encryption might have only been used by the kinds of highly motivated, sophisticated actors who were capable of developing or seeking it out

---

[3] *See, e.g.*, Eric Lichtblau & Joseph Goldstein, *Apple Faces U.S. Demand to Unlock 9 More iPhones*, N.Y. TIMES (Feb. 23, 2016), https://www.nytimes.com/2016/02/24/technology/justice-department-wants-apple-to-unlock-nine-more-iphones.html.

[4] *See* Jose Pagliery, *Apple Gets New Encryption Patent—Even as It Fights the FBI*, CNN (Mar. 18, 2016, 3:36 PM), http://money.cnn.com/2016/03/17/technology/apple-encryption-patent/index.html [https://perma.cc/NT3V-E4UY].

[5] *See* Justin (Gus) Hurwitz, *Encryption^{Congress}MOD (Apple + CALEA)*, 30 HARV. J.L. & TECH. 355, 399–402 (2017). This includes unbreakable encryption, phones that lock and delete data after a set number of unsuccessful log-on attempts, and communications platforms that retain no information at all. *See id.* at 403 & n.213; *see also* Cara McGoogan, *Revealed: The Most Secure Messaging Apps*, TELEGRAPH (U.K.) (Oct. 25, 2016, 12:22 PM), http://www.telegraph.co.uk/technology/2016/10/25/revealed-the-most-secure-messaging-apps/ [https://perma.cc/WZL2-DFXF] (describing communications platforms with end to end encryption and auto-deleting messages).

[6] *See* Hurwitz, *supra* note 5, at 357–58, 424.

[7] Valerie Caproni, the former general counsel for the FBI, described Internet providers as "promising their customers that they will thumb their nose at a U.S. court order." Charlie Savage, *U.S. Is Working to Ease Wiretaps on the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1. In the agency's view, companies can promise strong encryption so long as they can "figure out how they can provide us plain text." *Id.*

[8] Hurwitz, *supra* note 5, at 372.

[9] *See* 47 U.S.C. §§ 1001–1010 (2012); *see also* Hurwitz, *supra* note 5, at 356–57.

[10] Hurwitz, *supra* note 5, at 357.

themselves; they are unlikely to be affected by even a total ban on encryption.[11] But now, even low-tech people (like your narrator) are using encryption simply by virtue of having a relatively new iPhone, as "firms have begun incorporating very powerful encryption features into mass-market consumer-grade products and services."[12]

Now, practically unbreakable encryption is the norm, as Apple and Google have made it standard on all devices since 2014.[13] Apple has staked its reputation on this publicly, announcing that for all iPhones running iOS 8 and higher, the company "will not perform iOS data extractions [in response to government search warrants] as data extraction tools are no longer effective."[14] Apple never explained the irony of it being unable to extract data through its own actions. But while Apple may bear some responsibility for creating a system that it could not access itself, does that mean that the corporation should be statutorily tasked with undoing it?

This Essay takes the question of whether CALEA should be amended (or a new statute passed) as a starting point for a broader exploration of what assistance the government can justly ask of its citizens. There is a relative dearth of literature on the topic,[15] and I do not propose to resolve these issues within this Essay. I only hope to raise some questions that should be addressed in any project of legislative reform, particularly when that project contemplates imposing affirmative obligations of assistance on private parties who have no direct connection to government investigations.

---

[11] *See id.* at 402 ("Even if encryption software was outlawed, the underlying algorithms are already understood and widely available."). Hurwitz makes a helpful distinction between three categories of encryption users: first, people deemed to be threats to national security, who may be highly motivated to use encryption to further terrorist schemes; second, dissident minorities at risk of persecution by their government, who are highly motivated to escape government surveillance; and finally, ordinary criminals. *Id.* at 401–02.

[12] *Id.* at 415.

[13] *See* Devlin Barrett & Danny Yadron, *Phone Protections Alarm Law Enforcement: Moves by Apple and Google to Put Some Data Out of Reach of Police Are Latest Fallout from Snowden's Disclosures*, WALL ST. J., Sept. 23, 2014, at A4.

[14] *Legal Process Guidelines: U.S. Law Enforcement*, APPLE, at III. I. (Sept. 29, 2015), https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/RW8N-Z3W3]. The company added, "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.* Its current Legal Process Guidelines state, somewhat more apologetically, "Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key." *Legal Process Guidelines: Government & Law Enforcement Within the United States*, APPLE, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/U4RK-VAEY] (last visited Dec. 4, 2017).

[15] One of the few discussions of this issue in the literature is Jon C. Blue, High Noon *Revisited: Commands of Assistance by Peace Officers in the Age of the Fourth Amendment*, 101 YALE L.J. 1475 (1992) (arguing that laws requiring citizens to assist the police at possible physical risk to themselves are unconstitutional).

The current situation places the power to limit the scope of the government's investigative abilities, not with any branch of government, but with private corporations. In the name of the privacy and security of their customers, Apple and its counterparts have been able to render certain information effectively inaccessible, whether through encryption, password protection, or automatic file deletion.[16] Their new position as champions of privacy and bulwarks against government snooping may be based on deeply held beliefs. It may be based on market calculations. Apple has openly admitted in court filings that complying with court orders to assist in the execution of search warrants could "substantially tarnish the Apple brand."[17] But while it seems unlikely that the aim was to interfere deliberately with government investigations, that has been the result. How the dilemma should be resolved will depend upon one's view of the role of technology, the value of corporate autonomy, the necessity of criminal investigations and the power of search warrants.

Part I gives a brief sketch of the various statutes that touch on, but fail to govern these issues, and reviews the issues raised in the FBI-Apple litigation. Part II examines the three primary objections to updating CALEA to cover these questions, namely lack of necessity, futility, and threats to security. All of this leads us back, in Part III, to the question posed at the beginning: What help do private actors, not implicated directly in criminal or terrorist investigations, owe to the government?

I. AN UNSATISFYING STATUTORY LANDSCAPE

These issues all came to a head after the FBI obtained a warrant to search the smartphone of one of the people responsible for the December 2015 terrorist mass shooting in San Bernardino,[18] then found it was unable to unlock it.[19] The phone was an iPhone 5c, which was full-disk-encrypted, meaning that its data could only be accessed

---

[16] Obviously, some are alarmed by this development. *See* Cyrus R. Vance, Jr. et al., Opinion, *When Phone Encryption Blocks Justice*, N.Y. TIMES (Aug. 11, 2015), https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?mtrref=www.google.com&gwh=E26C36E29DA63582FC9B1C47EB3B2415&gwt=pay&assetType=opinion ("[I]n the absence of laws that keep pace with technology, we have enabled two Silicon Valley technology companies to upset that balance fundamentally.").

[17] Apple Inc.'s Response to Court's October 9, 2015 Memorandum and Order at 4, *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-01902-JO). Possibly realizing how mercenary this sounded, Apple followed up with a post on its website in which it claimed that its refusal to comply with government orders was "absolutely not" related to marketing or business strategy concerns. *Answers to Your Questions About Apple and Security*, APPLE, http://www.apple.com/customer-letter/answers [https://perma.cc/3E4P-7MM4] (last visited Dec. 4, 2017). "Nothing could be further from the truth," it added. *Id.*

[18] I decline to grant this individual the courtesy of naming him.

[19] Hurwitz, *supra* note 5, at 403.

with its user's individual passcode,[20] and which moreover could not be opened by a brute force attack or all the data would be wiped.[21] The government asked Apple for help, and the company refused, triggering a heated—and highly public—bout of litigation.[22] The district court granted the FBI a writ under the All Writs Act[23] (AWA) compelling Apple to assist in the execution of the search warrant.[24] But after Apple appealed, the government abruptly withdrew its petition when it reportedly paid an unnamed hacker to break into the phone.[25]

This dispute (which resulted in two magistrate judges reaching conflicting conclusions) revealed a statutory scheme ill-equipped to deal with the pace of technological change.[26] Certainly, none of the existing statutes said anything about accessing information on a physical device encrypted by a provider of information

---

[20] *See* Kristen M. Jacobsen, Note, *Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and Its Chilling Effect on Law Enforcement*, 85 GEO. WASH. L. REV. 566, 573 (2017). For an exquisitely technical explanation of full-disk encryption, see generally KAREN SCARFONE ET AL., NAT'L INST. OF STANDARDS & TECH., GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY § 3.1.1 (2007), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf [https://perma.cc/MT8E-E7G9].

[21] *See* Jacobsen, *supra* note 20, at 584–85 (describing brute force extraction and its limitations). The operating system automatically deletes all information after ten wrong password attempts. *Id.* at 585.

[22] *See id.* at 569. Apple CEO Tim Cook lost little time in writing an open letter to his customers, saying, "We feel we must speak up in the face of what we see as an overreach by the U.S. government. . . . [U]ltimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect." Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ [https://perma.cc/38X4-WNDG]. This earned him plaudits for being a champion of privacy. *See* Katie Benner & Nicole Perlroth, *How Tim Cook, In iPhone Battle, Became a Bulwark for Digital Privacy*, N.Y. TIMES (Feb. 18, 2016), http://www.nytimes.com/2016/02/19/technology/how-tim-cook-became-a-bulwark-for-digital-privacy.html?mcubz=3. For a good recounting of the facts of the litigation, see Jacobsen, *supra* note 20, at 568–69.

[23] *See* 28 U.S.C. § 1651 (2012).

[24] *See* Eric Lichtblau, *Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman*, N.Y. TIMES (Feb. 16, 2016), http://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html.

[25] *See* Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html. Reuters reported that the assistance came from an Israeli forensics company, Cellebrite. *See Israeli Firm Helping FBI to Open Encrypted iPhone: Report*, REUTERS (Mar. 23, 2016, 6:55 AM), http://www.reuters.com/article/us-apple-encryption-cellebrite-idUSKCN0WP17J [https://perma.cc/RC46-KKXE].

[26] As one student puts it, courts face difficulty "applying the limited and antiquated statutes and case law surrounding this issue." John Mylan Traylor, Note, *Shedding Light on the "Going Dark" Problem and the Encryption Debate*, 50 U. MICH. J.L. REFORM 489, 503 (2017).

services. The Communications Assistance for Law Enforcement Act (CALEA) covered telecommunications carriers, but not providers of information services.[27] The Stored Communications Act (SCA) did cover information service providers, but only applied to the content of communications, such as emails, held by third parties, not stored on an individual's smartphone.[28] CALEA imposed affirmative duties on telecommunications carriers to assist law enforcement in conducting wiretaps and pen registers, but specifically exempted encryption from its reach.[29]

Apple, in short, was not the type of entity meant to be covered by CALEA,[30] and the government's requested order had nothing to do with wiretapping. Indeed, the whole reason that the FBI was forced to dust off the All Writs Act, enacted in 1789, was that none of the existing statutes seemed to cover their specific situation.[31] But because CALEA is one of the few statutes to impose an affirmative duty to assist in government investigations, and the AWA can be used to compel third parties to act, the following section will examine them both.

A. CALEA: An Explicit Imposition of Duty

As mentioned above, CALEA was enacted at a time of technological change in telecommunications, which affected the government's ability to conduct wiretaps.[32] In the old days, wiretapping was almost laughably low-tech, since "[f]irst[-]generation wiretaps were conducted through copper telephone wires by simply touching a separate copper wire against the phone line running from [a suspect's] house to the local phone company."[33] As these copper wires were replaced by fiber optic cables, the old wiretap technology became less useful.[34] The government raised the alarm

---

[27] *See* 47 U.S.C. § 1002(b)(2) (2012) (clarifying that 47 U.S.C. § 1002(a) does not apply to information services or equipment facilities).

[28] *See* 18 U.S.C. §§ 2701–2712 (2012).

[29] *See* 47 U.S.C. § 1002(b)(3).

[30] In fact, Apple specifically referred to itself as an entity that provides information services, rather than as a telecommunications provider. *See* Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 8 n.13, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-cm-00010-SP (C.D. Cal. Feb. 25, 2016) [hereinafter Apple Inc.'s Motion to Vacate Order]. This seems like a fair characterization.

[31] *See* Traylor, *supra* note 26, at 505.

[32] Hugh J. McCarthy, *Decoding the Encryption Debate: Why Legislating to Restrict Strong Encryption Will Not Resolve the "Going Dark" Problem*, J. INTERNET L., Sept. 2016, at 1, 20 (discussing CALEA as a response to the development of fiber optic cables).

[33] *Id.*

[34] *See* Peter Swire & Kenesa Ahmad, *'Going Dark' Versus a 'Golden Age for Surveillance,'* CTR. FOR DEMOCRACY & TECH. (Nov. 28, 2011), https://cdt.org/blog/%E2%80%98

that it was "going dark," losing the ability to wiretap suspects.[35] In response, Congress passed CALEA,[36] which ensured that telecommunications companies would continue to provide investigative agencies with the technological resources they needed to maintain their investigations.[37]

CALEA, which can most charitably be described as "exceptionally technical,"[38] is a fairly limited statute: its only brief was to preserve the government's ability to conduct wiretaps and obtain pen registers,[39] leaving developing technologies for another day. It therefore imposed an obligation on any telecommunications carrier to "ensure that its equipment, facilities, or services" remained capable of "enabling the government, pursuant to a court order or other lawful authorization, to intercept . . . all wire and electronic communications" transmitted by that carrier.[40] The statute also imposed an obligation that telecommunications carriers maintain the ability to enable the government to obtain pen registers.[41]

Beyond that, the statute explicitly barred the government from requiring or banning any particular design feature in the carrier's equipment or services.[42] This way, the companies could run their service however they wanted, so long as the government's ability to wiretap[43] was not adversely affected. This was in marked contrast

---

going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/ [https://perma.cc/2P2Z-KX2V].

[35] *See id.*

[36] *See* H.R. REP. NO. 103-827(I) [hereinafter CALEA HOUSE REPORT], pt. 1, at 9 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489 (explaining that CALEA's purpose was "to preserve the government's ability . . . to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services").

[37] *Id.* at 3489–90. Wiretaps record conversations that take place over a tapped phone, while pen registers record the numbers called by a given telephone, but do not divulge any content. Hurwitz, *supra* note 5, at 362.

[38] Hurwitz, *supra* note 5, at 373.

[39] CALEA was "intended to preserve the status quo . . . to provide law enforcement no more and no less access to information than it had in the past." CALEA HOUSE REPORT, *supra* note 36, at 3502.

[40] 47 U.S.C. § 1002(a)(1) (2012).

[41] *Id.* § 1002(a)(2). This section also exempts "any information that may disclose the physical location of the subscriber." *Id.* § 1002(a)(2)(B).

[42] *Id.* § 1002(b)(1)(A)–(B) (providing that no law enforcement agencies or officers may "require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service" nor "prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service").

[43] For the purposes of the CALEA discussion, I am including the obtaining of pen registers under this term for convenience sake. *See* CALEA HOUSE REPORT, *supra* note 36, at 3490.

to early drafts of the Act, "which would have barred introduction of services or features that could not be tapped."[44]

CALEA also expressly exempted "information services" from its reach,[45] which meant that, at least initially, the Act did not apply to Internet Service Providers.[46] As noted above, the SCA does cover information service providers,[47] but only applies to the content of communications, and then only when the communications are held by third parties on remote servers.[48] It sheds no light on the problem of accessing an encrypted device, or communications saved by parties to the communications.[49]

Finally, and of particular interest to Apple, CALEA explicitly protected telecommunications companies from being forced to decrypt "or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer."[50] There was only one situation in which a carrier could be compelled to assist in decrypting a communication, and that was when "the encryption was provided by the carrier

---

[44] *Id.* at 3499.

[45] § 1002(b)(2)(A). CALEA defined "information services," fairly unhelpfully, as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and includes a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; electronic publishing; and electronic messaging services." 47 U.S.C. § 1001(6)(A)–(B) (2012) (internal subsection markers omitted). The definition of "telecommunications providers" was later extended by the FCC to include broadband providers and VoIP (voice over Internet protocol) platforms such as Skype. *See* Am. Council on Educ. v. FCC, 451 F.3d 226, 227 (D.C. Cir. 2006). This interpretation was ruled a "reasonable policy choice" by the District of Columbia and Third Circuit Courts of Appeals. *See* Time Warner Telecom, Inc. v. FCC, 507 F.3d 205, 220 (3d Cir. 2007); *Am. Counsel on Educ.*, 451 F.3d at 232.

[46] *See* § 1002(b)(2); Deborah F. Buckman, Annotation, *Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use*, 15 A.L.R. Fed. 2d 537, § 2 (2006) ("It is noteworthy that CALEA does not cover 'information services' such as e-mail and Internet access.").

[47] *See* 18 U.S.C. § 2702(a)(1)–(2) (2012); *In re* Order Authorizing Prospective & Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889, 892 n.11 (S.D. Tex. 2014) ("The SCA 'only regulates information pertaining to customers or subscribers of covered information services.'" (quoting Nathaniel Gleicher, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1947 (2009))). *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

[48] *See* RICHARD M. THOMPSON II & JARED P. COLE, CONG. RESEARCH SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) 1 (2015) (giving examples, such as Google turning over emails or Facebook providing private posts).

[49] *Id.* at summary (noting that the SCA "does not apply to government access to records held by a party to the communication").

[50] § 1002(b)(3).

and the carrier possesses the information necessary to decrypt the communication."[51] The exemption for encryption, it turns out, was based on a government miscalculation.

The initial draft of CALEA "imposed substantial limits on the use of encryption by telecommunications carriers."[52] But this proposal faced considerable opposition,[53] while in the meantime, the government had developed what it believed to be a viable backdoor into encrypted communications in the form of an "escrowed encryption standard" that was to be housed in a low-cost microchip.[54] This microchip, known as the "Clipper Chip," would have been included in all commercial electronics.[55] In order to avoid a costly legislative fight, and because they thought a practical solution had been found, the FBI and Congress agreed to put off legislation on encryption until a later date.[56] Encryption by telecommunications carriers was therefore kept out of the requirements of CALEA.

Unfortunately for the government, the Clipper Chip "was shown to have significant design flaws that rendered it insecure"—a costly and embarrassing setback.[57] Meanwhile, CALEA did nothing to help law enforcement deal with the increasing use and growing strength of encryption. Therefore, cautions Gus Hurwitz, it is incorrect to read the statute as specifically endorsing encryption.[58] In fact, he argues that "the

---

[51] *Id.* The CALEA House Report similarly noted that "telecommunications carriers have no responsibility to decrypt encrypted communications . . . unless the carrier provided the encryption and *can* decrypt it." CALEA HOUSE REPORT, *supra* note 36, at 3504 (emphasis added). In other words, this requirement did not "prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access." *Id.* Steven Morrison points out that there is considerable ambiguity in the phrase, "possesses the information necessary to decrypt the communication," because it could suggest either present possession of existing code that could decrypt the communication, or "possession of the knowledge and technological ability to develop the code." Morrison, *supra* note 1, at 2067 (emphasis omitted in first quote). Conceivably, Apple "possesses the information" necessary to decrypt if the term "possess" is understood as "having the technological savoir faire and know-how" to develop the necessary code to decrypt, as opposed to already having the code on hand. *See id.* Under that reading, most telecommunications companies, including Apple, if it was so designated, would be on the hook even under CALEA.

[52] Hurwitz, *supra* note 5, at 369.

[53] *See, e.g.*, HAL ABELSON ET AL., THE RISKS OF KEY RECOVERY, KEY ESCROW, AND TRUSTED THIRD-PARTY ENCRYPTION 19 (1997) (arguing that mandatory key recovery systems are "less secure, more costly, and more difficult to use").

[54] Hurwitz, *supra* note 5, at 406.

[55] *See id.*

[56] *See id.* at 407–08 ("The FBI believed that it had a workable escrow standard that mooted the need to address encryption at the time CALEA was adopted.").

[57] *Id.* at 407.

[58] *Id.* at 408. Because the omission was deliberate, writes Hurwitz, "it is factually wrong to say that CALEA addressed encryption in any direct or meaningful way—let alone that it is a blanket expression of congressional approval for the use of encryption." *Id.*

only thing that CALEA can tell us about Congress's views toward encryption is that Congress has concerns about encryption but doesn't know what to do about them."[59]

So CALEA's lessons on encryption are debatable at best, and did not really address the sort of issues raised by the Apple dispute—accessing the data on a physical device in the custody of the government. What is significant about the statute is that it imposes an affirmative obligation on private actors to shape their commercial and technological behavior in a way that can assist the government, while at the same time forbidding the government to dictate any particular design—two aims that seem in tension. While there are plenty of statutes that require compliance with law enforcement on the behalf of private parties—complying with subpoenas and warrants, rendering the technical assistance to initiate and maintain a wiretap—CALEA represents a difference in kind. Unlike the Wiretap Act[60] (or the duty to hand over your clients' bank records), CALEA "imposes an affirmative ex ante obligation on third parties to design their systems so as to be capable of providing such assistance in the future."[61]

B. Apple and the FBI Meet the All Writs Act

The story of Apple's relationship with the FBI has the tang of a romance gone sour. According to a report issued by the Manhattan District Attorney, up until recently, Apple cooperated quite well with the government.[62] The report reminisces how Apple was able to tout its user security and still "maintain[ ] the ability to help 'police investigating robberies and other crimes, searching for missing children, trying to locate a patient with Alzheimer's disease, or hoping to prevent a suicide.'"[63] During that period, prosecutors' offices were able to get search warrants coupled with "unlock orders" that required the companies to assist in data extraction procedures.[64] "Then, without explanation," the report says, "Apple changed its position and refused

---

[59] *Id.*

[60] *See* 18 U.S.C. § 2518(4) (2012) (stating that third parties served with an order under the Wiretap Act "shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception").

[61] Hurwitz, *supra* note 5, at 409. Hurwitz goes on to argue that this is not as unusual as it seems, as legislatures "frequently impose design obligations [in building or banking] in order to stave off foreseeable future problems." *Id.* But it seems to me that there is a difference between mandating that entry points on a building comply with the ADA and telling companies that they cannot build their most profitable and popular structures in the first place.

[62] *See* MANHATTAN DIST. ATTORNEY'S OFFICE, SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 19 (2016) [hereinafter DA REPORT].

[63] *Id.* at 13 (citing *Apple's Commitment to Customer Privacy*, APPLE (June 16, 2013), https://www.apple.com/apples-commitment-to-customer-privacy/ [https://perma.cc/9YKK-MW7W]).

[64] *See* Jacobsen, *supra* note 20, at 587 (citing DA REPORT, *supra* note 62, at 4).

to comply with court-issued extraction orders, regardless of the operating system running on the device."[65]

After the San Bernardino terrorist attack, the government asked Apple for help in breaking into the perpetrator's iPhone, but Apple refused, claiming that it could not comply with the order without creating code that would jeopardize the privacy protections of its millions of customers.[66] Because, in the government's view, CALEA did not apply to a situation involving the decryption of a physical device, the government turned to the AWA, part of the Judiciary Act of 1789, which provides that district courts can "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[67] In this case, the government had a valid search warrant based on probable cause, issued by a court, but it was unable to execute it. The government therefore argued that the court could thus issue a writ compelling Apple to help the FBI to execute the warrant.[68] The United States District Court for the Central District of California issued the writ, and Apple appealed.[69] After some heated motion practice, the FBI abruptly withdrew its request, having found an alternative way to crack the phone.[70]

But the case raised some unresolved questions about the reach of the statutory scheme: whether it covered tech giants like Apple and Google, and whether it left room for the AWA to play a role. This is because the AWA is most properly seen as a gap-filling measure, a way "to fill[ ] the interstices of federal judicial power when those gaps threaten[ ] to thwart the otherwise proper exercise of federal courts' jurisdiction."[71] Apple argued that the AWA could not apply where Congress had already spoken.[72] The duties imposed on companies by CALEA were similar to the task requested by the government, but information services companies such as Apple were explicitly exempted from their reach.[73] And because the statute forbid the

---

[65] *See* DA REPORT, *supra* note 62, at 19.

[66] *See* Apple Inc.'s Motion to Vacate Order, *supra* note 30, at 7.

[67] 28 U.S.C. § 1651(a) (2012). This request was factually unprecedented; as the Supreme Court had earlier noted, "it [wa]s difficult to conceive of a situation in a federal criminal case today where [an AWA writ] would be necessary or appropriate." Carlisle v. United States, 517 U.S. 416, 429 (1996) (quoting United States v. Smith, 331 U.S. 469, 475 n.4 (1947)).

[68] *See* 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 at 3, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 15-0451M (C.D. Cal. Feb. 16, 2016).

[69] *See generally* Apple Inc.'s Motion to Vacate Order, *supra* note 30.

[70] *See* Hurwitz, *supra* note 5, at 404.

[71] Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 41 (1985).

[72] *See* Apple Inc.'s Motion to Vacate Order, *supra* note 30, at 15–19.

[73] As Steven Morrison points out, "[E]ven if CALEA did govern information service providers, Congress specifically exempted only telecommunications carriers from the duty to decrypt—it could have, but did not, exempt information service providers." Morrison, *supra*

government from imposing design features or limiting encryption, similar requests could not be granted under the AWA.[74] Conveniently, Apple was not a telecommunications provider, so the affirmative part of the statute did not apply.

The magistrates who were asked to apply the AWA did not have a large body of doctrine to draw on. The Supreme Court had addressed the application of the AWA, and concomitantly the legality of imposing affirmative duties on third parties, in *United States v. New York Telephone Co*.[75] That case arose in the late 1970s, when the FBI was investigating an illegal gambling ring on East 14th Street in Manhattan and obtained a court order authorizing the installation of two pen registers.[76] At that time, pen registers were mechanical devices that had to be literally attached to the target's telephone line.[77] Because the devices would have been visible to an alert observer[78] and the agency did not want to tip off the targets of the investigation, it asked New York Telephone to lease two additional telephone lines so the pen registers could be installed some distance away from the target location.[79] For reasons that remain obscure, the phone company "refused to lease lines to the FBI which were needed to install the pen registers in an unobtrusive fashion."[80] Instead, the company "advised the FBI to string cables from the 'subject apartment' to another location where pen registers could be installed."[81]

---

note 1, at 2071. If so, he argues, "CALEA's protection of telecommunications carriers from any duty to decrypt does not extend to information service providers." *Id.* at 2072. So, if only telephone companies are exempt from the duty to decrypt (except under certain specific, not-fully understood conditions), then presumably such a duty could be imposed on information service providers. *See id.* at 2071–72.

[74] *See id.* at 2063–64.

[75] 434 U.S. 159 (1977).

[76] *See id.* at 161–62.

[77] *See id.* at 161 n.1.

[78] *Pen Register*, WIKIPEDIA, https://en.wikipedia.org/wiki/Pen_register [https://perma.cc/V92Q-Z6FX] (last visited Dec. 4, 2017) (citing U.S. Patent No. 1647 (issued June 20, 1840)) ("The term *pen register* originally referred to a device for recording telegraph signals on a strip of paper. Samuel F.B. Morse's 1840 telegraph patent described such a register as consisting of a lever holding an armature on one end, opposite an electromagnet, with a fountain pen, pencil or other marking instrument on the other end, and a clockwork mechanism to advance a paper recording tape under the marker.").

[79] *See* Jack Pringle, *From Breaking Down Doors to Building Back Doors: The FBI-Apple Case Is Only the Latest Battle Pitting Privacy Against the Need to Investigate Crime*, S.C. LAW., Jan. 2017, at 34, 38–39.

[80] *N.Y. Tel.*, 434 U.S. at 162.

[81] *Id.* at 163. This was not terribly helpful, since "because of the location of the apartment and because the suspects were known to use counter-surveillance techniques, the FBI determined that 'if men were observed stringing lines and cables from the subject apartment to another location, the gambling operation would cease to function.'" Brief for the United States at 9, *N.Y. Tel.*, 434 U.S. 159 (No. 76-835) (internal citations omitted). So some poor FBI agent had to canvass the neighborhood for four days, looking for a "location where [the

The FBI successfully sought a writ obliging assistance under the AWA.[82] New York Telephone defended its position on the basis that, because the pen register application was not attached to a Title III wiretap order, it was under no obligation to provide assistance.[83] In determining whether it was proper to issue a writ under the AWA,[84] the Supreme Court effectively considered three factors that were later distilled as:

> 1. the closeness of the relationship between the person or entity to whom the proposed writ is directed and the matter over which the court has jurisdiction;
> 2. the reasonableness of the burden to be imposed on the writ's subject; and
> 3. the necessity of the requested writ to aid the court's jurisdiction . . . .[85]

It reasoned that New York Telephone was not too far removed from the controversy, that the burden on it was not unreasonable, and that the FBI would have been effectively barred from installing a useful pen register without the company's assistance.[86] Therefore, the AWA did allow the order.[87]

What is notable is that the Court reversed a ruling of the appellate court that it interpreted as "generally barring district courts from ordering any party to assist in the installation or operation of a pen register."[88] Justice White, writing for the majority, seemed unmoved by arguments that an order demanding assistance in installing a pen register "pose[d] a severe threat to the autonomy of third parties who for whatever reason prefer not to render such assistance."[89] On the contrary, not forcing them to comply, he wrote, "would frustrate the clear indication by Congress

---

agency] could string its own wires and attach the pen registers without alerting the suspects." *Id.* He didn't find one. *N.Y. Tel.*, 434 U.S. at 163.

[82] *See N.Y. Tel.*, 434 U.S. at 163.

[83] *Id.*

[84] While the district court issued a writ under the AWA ordering the phone company to comply with the pen register order, the Court of Appeals for the Second Circuit reversed, "express[ing] concern that 'such an order could establish a most undesirable, if not dangerous and unwise, precedent for the authority of federal courts to impress unwilling aid on private third parties.'" *Id.* at 164 (quoting Application of United States *in re* Pen Register Order, 538 F.2d 956, 962–63 (2d Cir. 1976)).

[85] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 351 (E.D.N.Y. 2016).

[86] *See N.Y. Tel.*, 434 U.S. at 174–75.

[87] *Id.* at 176–78.

[88] *See id.* at 171.

[89] *Id.*

that the pen register is a permissible law enforcement tool by enabling a public utility to thwart a judicial determination that its use is required."[90]

The power conferred by the AWA, concluded the Court, allowed a court to dictate "to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice."[91]

While the magistrate judge presiding over the Apple case in California followed *New York Telephone* in issuing a writ under the AWA, in a similar case in the Eastern District of New York, a magistrate judge declined to do so. That court considered a request pursuant to the AWA for assistance in breaking into a suspect's password-protected iPhone, but ruled that it could not use the AWA because CALEA was part of a comprehensive statutory scheme that left no gaps.[92]

The AWA, reasoned the court, could neither be "interpreted to empower courts to do something that another statute already authorizes (but that might have threshold requirements that cannot be satisfied in the circumstances of a particular case),"[93] nor be used "to issue an order that is explicitly or implicitly prohibited under a federal statute."[94] Taking CALEA and the SCA together, the New York court found "a comprehensive legislative scheme" that prevented use of the AWA.[95] Specifically, the court found that "[t]he absence from that comprehensive scheme of any requirement that Apple provide the assistance sought here implies a legislative decision to prohibit the imposition of such a duty."[96] This is not entirely persuasive. This argument assumes that Congress in 1994, over two decades before the launch of the iPhone, had envisaged the difficulties of breaching the encryption on such a device, and decided to prohibit it.

---

[90] *Id.* at 178.

[91] *Id.* at 174 (internal citations omitted).

[92] *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 357 (E.D.N.Y. 2016). The court noted that although CALEA did not regulate data at rest, the Stored Communications Act (SCA) did. *See id.* at 355–56 (citing 18 U.S.C. § 2703(f)(1) (2012)). But none of the SCA's provisions "imposed any obligation on Apple to provide the assistance at issue," and "CALEA expressly stated that the assistance requirement did not apply to 'information services.'" *Id.* at 356 (footnote omitted) (citing 47 U.S.C. § 1002(b)(2)(A)).

[93] *Id.* at 353.

[94] *Id.*

[95] *Id.* at 357. The flaw in this argument is that it converts a political compromise to defer issues of encryption into an active commitment to protect encryption, in other words, "a legislative choice to exempt tech companies from complying with unlock orders for encrypted smartphones." Jacobsen, *supra* note 20, at 589. Hurwitz argues compellingly that it was no such thing. *See* Hurwitz, *supra* note 5, at 376–85; *see also* Morrison, *supra* note 1, at 2075.

[96] *In re Apple*, 149 F. Supp. 3d at 357.

The AWA remains a vehicle that several courts have used to compel innocent third parties to assist law enforcement.[97] But even if a consensus develops that the AWA may be used to compel assistance, courts would still have to decide on a case-by-case basis whether a requested order was agreeable to the usages and principles of law.

Attempting to balance the interests in law enforcement, privacy, and private business goals in each individual situation as part of an ad hoc series of judicial decisions would be costly and inefficient. Companies might end up with different results in different jurisdictions (as Apple nearly did), creating uncertainty. In fact, there seems to be a consensus that Congress needs to step in and make a decision on encryption.[98] It is to that possibility that we now turn.

II. SHOULD CALEA BE AMENDED?

Should Congress pass or amend law that specifically allows courts to issue orders of assistance like that in the Apple case, or even that would mandate such assistance directly? While a statute of general application would answer some of the constitutional issues in the California Apple case, there is still plenty of resistance to the idea of amending or supplementing the Communications Assistance for Law Enforcement Act (CALEA). Overall, the arguments against legislation come down to the following three objections: it would be unnecessary, it would be futile, and it would be unsafe. Unnecessary, because we are currently in a golden age of surveillance, so the government has nothing to complain about. Futile, because

---

[97] *See, e.g.*, Klay v. United Healthgroup, Inc., 376 F.3d 1092, 1100 (11th Cir. 2004) (observing that a court may issue an AWA injunction against anyone, including a non-party, who is "in a position to frustrate the implementation of a court order or the proper administration of justice, . . . even those who have not taken any affirmative action to hinder justice" (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977))); United States v. City of Detroit, 329 F.3d 515, 517 (6th Cir. 2003) (holding that the AWA permits district courts "to bind nonparties in order to prevent the frustration of consent decrees that determine parties' obligations under the law"); United States v. Int'l Bhd. of Teamsters, 266 F.3d 45, 50 (2d Cir. 2001) ("The [AWA]'s grant of authority is plainly broad and, on its face, makes no distinctions between parties and nonparties."); Yonkers Racing Corp. v. City of Yonkers, 858 F.2d 855, 863 (2d Cir. 1988) (holding that the AWA authorizes action against a non-party to the original action in "exceptional circumstances" in which the non-parties "are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice" (internal quotations and emphasis omitted) (quoting Benjamin v. Malcolm, 803 F.2d 46, 53 (2d Cir. 1986))).

[98] *See, e.g.*, Hurwitz, *supra* note 5, at 411–12; Jacobsen, *supra* note 20, at 599–600; Morrison, *supra* note 1, at 2081–82; Traylor, *supra* note 26, at 512–15. It certainly would be helpful if Congress clarified matters, although given how dysfunctional the chambers have become, this solution might not be forthcoming anytime soon.

if rules against unbreakable encryption are enforced in the United States, the bad guys will just switch to evanescent technologies or servers in Kazakhstan. Unsafe, because any access will effectively mandate a backdoor that will jeopardize the privacy of millions for the sake of investigating a handful of malefactors. There are doubtless additional arguments to be made,[99] but I will focus on these three.

A. Necessity and Futility

The first question is whether all this is necessary. Privacy advocates argue that there is no real need for government access to encrypted devices. One plausible argument against Congressional action is that, far from "going dark," we are actually in a "golden age of surveillance."[100] Some commentators point to all the various sources of information now available—"granular location information," vast networks of associates, viewing and reading habits, in short, everything that constitutes the ever-growing "'digital dossiers' about individuals' lives"—and conclude that "[c]ompared with earlier periods, surveillance capabilities have greatly expanded."[101]

Matt Olsen, Bruce Schneier, and Jonathan Zittrain point to several other features of technology that suggest that one type of surveillance may be replaced by another.[102] The "Internet of Things" would seem to offer multiple possibilities for surveillance as the objects people interact with every day could be commandeered by law enforcement.[103] Encryption itself has natural limits, since the business model of most companies requires them to retain enough access to users' information to bombard them with tailored ads.[104] The ability to map people's contacts on social media and build sophisticated networking models is a relatively new phenomenon.[105] So the loss of agency access because of encryption may be marginal, and "more than offset by surveillance gains from computing and communications technology."[106]

Still, while there is indeed more information available than ever before, this new information does not precisely supplant the lost information.[107] There is a wide

---

[99] A few that come to mind are reliance, in that it would be unfair to amend CALEA after companies—and their customers—have gotten used to unbreakable encryption; loss of market share; and so forth.

[100] Swire & Ahmad, *supra* note 34.

[101] *Id.*

[102] *See* MATT OLSEN ET AL., BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. U., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 9–10, 12 (2016), https://cyber.harvard.edu/publications/2016/Cybersecurity/Dont_Panic [https://perma.cc/AX5T-NRT8].

[103] *See id.* at 12–15.

[104] *See, e.g.*, Rolfe Winkler & Jack Marshall, *Google Imitates Facebook with Email Marketing*, WALL ST. J., Apr. 15, 2015, at B4.

[105] *See* Simeon Edosomwan et al., *The History of Social Media and Its Impact on Business*, 16 J. APPLIED MGMT. & ENTREPRENEURSHIP 79 (2011).

[106] *See* Swire & Ahmad, *supra* note 34.

[107] *See* Hurwitz, *supra* note 5, at 400–01.

variety of relevant information that can only be found on a physical smartphone.[108] If the phone's user is unavailable or uncooperative,[109] law enforcement hits a dead end. The Manhattan District Attorney's Office noted that, in its office alone, there were hundreds of cases adversely affected because of lawfully seized iPhones and iPads that remained unsearchable.[110]

On the other hand, Apple's defenders argue that any attempt to require assistance would push toward creating a backdoor that Apple, many in the tech industry, and even many in government, oppose.[111] It could also be very costly to targets of such orders, like Apple, both in terms of labor required to comply and their loss of market share against foreign companies who may retain strong encryption and who are not within the reach of such orders.[112] Access could also tarnish Apple's brand.[113]

---

[108] This includes "iMessage content and details (e.g., dates, times, phone numbers involved), SMS/MMS content, historical cell site data, historical GPS data, contacts, photos/videos, internet search history, internet bookmarks, and third-party app data." Jacobsen, *supra* note 20, at 578 (other internal citations omitted) (citing DA REPORT, *supra* note 62, at 6–8). Jacobsen also reviews the reasons why access to the cloud accounts of suspects might not provide the same information as that on the smartphone itself. *See id.* at 579–81.

[109] Whether users are protected from being compelled to divulge their passcodes by the Fifth Amendment is still up for dispute. For a discussion of this, see generally Caren Myers Morrison, *Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment*, 65 ARK. L. REV. 133, 134 (2012).

[110] *See* DA REPORT, *supra* note 62, at 8 (noting that there were 423 phones and tablets in its custody that could not be accessed).

[111] Nick Wingfield & Mike Isaac, *Apple Letter on iPhone Security Draws Muted Tech Industry Response*, N.Y. TIMES (Feb. 18, 2016), https://www.nytimes.com/2016/02/19/technology/tech-reactions-on-apple-highlight-issues-with-government-requests.html.

[112] *See, e.g.*, Brief of *Amici Curiae* Electronic Frontier Foundation and 46 Technologists, Researchers, and Cryptographers, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 16-cm-00010-SP (C.D. Cal. Mar. 3, 2016). The Electronic Frontier Foundation's (EFF) amicus brief argued that the requested order would have required Apple to draft code and then electronically sign the code, signaling Apple's trust in the code and "its endorsement and stamp of approval." *Id.* at 4. The EFF described this as compelled speech that would force Apple "to express itself in conflict with its stated beliefs." *Id.* at 7. A number of amici for Apple expressed concern that the requested order would undermine Apple's business model, and Apple raised arguments that forcing its engineers to write code at the government's behest would be conscription "on a mission that is contrary to the values of the company and these individuals." Apple Inc.'s Reply to Government's Opposition to Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search at 25, *In re Search of an Apple iPhone*, No. CM 16-10 (SP) (Mar. 15, 2016). For a discussion of the Lochnerian arguments and Thirteenth Amendment ramifications, see Morrison, *supra* note 1, at 2078–79.

[113] Whether most consumers would care is another matter. *See* Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/H9ZS-R3WM] (noting that "Americans express a consistent lack of confidence about the security of everyday communication channels and the organizations that control them").

Finally, without a new statute or amendment, would the government really be any worse off? In the earliest days of organizational investigations, communications most often took place face-to-face, and there was no lasting evidence of who had met with whom, or what was said.[114] The best information in those days was obtained by engaging the cooperation of co-conspirators. The use today by some malefactors of the types of evanescent messaging that leave no trace is not so different—in the absence of an informant, the information is beyond reach. But psychologically, it is hard to accept the loss of something that was yours, however briefly.[115]

In the meantime, arguments abound about the ways malefactors can easily migrate to non-American-made encryption technology, or use messaging apps that retain no more information than a face-to-face conversation, making any legislation essentially pointless.

B. Security

Probably the most compelling argument that access should not be legislated is that it would be unsafe. The "Keys Under Doormats" group argues vigorously that mandating a backdoor would lead to widespread harm.[116] In its view, weakening encryption is tantamount to banning it altogether.[117] On the other hand, at least one proposal has been made that appears to have potential.[118] Matt Tait, an information security specialist, proposes a modification to Apple's Cloud Key Vault, currently

---

[114] The notorious mafia "walk-talks," whereby mobsters took walks with confederates to escape bugging by law enforcement, are a prominent example of this. *See* GENE MUSTAIN & JERRY CAPECI, MOB STAR: THE STORY OF JOHN GOTTI 300–01 (1988).

[115] Cognitive psychologists refer to this as the "endowment effect," which is the phenomenon of valuing what you have over something comparable that you do not, and "loss aversion," which is the impulse not to lose what you already have, even if it is replaced by something of similar value. *See generally* Daniel Kahneman et al., *Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias*, 5 J. ECON. PERSP. 193 (1991).

[116] *See* HAROLD ABELSON ET AL., COMPUT. SCI. & ARTIFICIAL INTELLIGENCE LAB., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS 1–3, 10 (2015), https://dspace.mit.edu/handle/1721.1/97690 [https://perma.cc/CYQ2-A8RS].

[117] *See, e.g.*, *id.* at 2–3; ABELSON ET AL., *supra* note 53, at 6–7; Michael A. Specter, *Apple's Cloud Key Vault, Exceptional Access, and False Equivalences*, LAWFARE (Sept. 7, 2016, 11:06 AM), https://www.lawfareblog.com/apples-cloud-key-vault-exceptional-access-and-false-equivalences [https://perma.cc/3ANB-5A9J].

[118] The Manhattan DA likes the proposal: "One technologist has proposed a method that would provide secure, lawful access to phones' contents by placing the filesystem key that can decrypt data on the phone in a series of *cryptographic envelopes* that, like Russian dolls, are 'nested,' one envelope inside the other." *See* DA REPORT, *supra* note 62, at 15 (citing Matt Tait, *An Approach to Jim Comey's Technical Challenge*, LAWFARE (Apr. 27, 2016, 7:00 AM), https://www.lawfareblog.com/approach-James-Comeys-technical-challenge [https://perma.cc/3AEM-22T7]).

their newest form of crypto-security.[119] In August 2016, Apple announced that it had developed the Cloud Key Vault, which Tait describes as "the very thing that they and the privacy community have been saying for years is reckless, dangerous or impossible: a high-value encryption key secured in a vault such that the key can't be stolen or misused by hackers or malicious insiders."[120]

Prior to the Cloud Key Vault, one of the ways that Apple kept users' data secure was through its "Secure Enclave" processor, which would permanently lock a device after ten unsuccessful password entry attempts—indeed, this was what prevented the FBI from mounting a "brute force" attack on the San Bernardino iPhone.[121] Apple then developed the iCloud keychain, which enabled users to automatically synchronize their saved passwords across other Apple devices, but encrypts those passwords before uploading them.[122] And in order to protect those encrypted passwords now uploaded to the Cloud, it developed the Cloud Key Vault, which Tait describes as a kind of "enormous Secure Enclave for the entire iCloud data-center," managing the number of PIN guesses and "ensur[ing] that after ten failed PIN guesses, the data in the encrypted keychain file becomes permanently inaccessible."[123]

But the company still faced two vulnerabilities in the face of hackers and law enforcement subpoenas: the fact "that the attacker could get ahold of the master encryption key hidden inside the Cloud Key Vault," and its own ability to upload new code to the Vault itself that could disable or reset the password attempt counter so that government agencies could discover PINs by brute force.[124] Apple's solution was to destroy its access to the Vault in such a way that once the access is destroyed "Cloud Key Vault operates entirely autonomously according to the code written at the time when it started."[125]

And because that code cannot be tampered with or changed without destroying the contents, Apple had basically found a solution to the often-used argument that

---

[119] *See* Matt Tait, *Apple's Cloud Key Vault and Secure Law Enforcement Access*, LAWFARE (Sept. 14, 2016, 10:09 AM), http://www.lawfareblog.com/apples-cloud-key-vault-and-secure-law-enforcement-access [https://perma.cc/RF9R-ZQA4]. I hasten to add that the technical ramifications of these arguments are above my pay grade, so I am going to assume that Tait knows what he is talking about.

[120] Matt Tait, *Apple at BlackHat: Reopening the "Going Dark" Debate*, LAWFARE (Aug. 12, 2016, 9:42 AM), https://lawfareblog.com/apple-blackhat-reopening-going-dark-debate [https://perma.cc/C46V-GM4U].

[121] *See id.*

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Id.* As Tait explains, "Apple employees have no administrative access to the device. They cannot reach in and take out the master encryption key. They cannot reach in and reset the 'failed PIN-guess' counter on any file. They cannot even upload new code to the device," because doing so would trigger "the destruction of the master-key, thereby causing the cryptographic self-destruction of all of the uploaded keychain files." *Id.*

"the technology community simply does not know how to securely store high-value encryption keys such that they can be used, but can't be stolen or misused by hackers or malicious insiders."[126] Or, for that matter, by the government.

According to Tait, this creates a conundrum for Apple. Ordinarily, he explains, tech companies' reasons for not being able to assist law enforcement in executing search warrants or responding to subpoenas "boil down to 'sorry, we don't have the content' or 'sorry, we don't have the keys.' But this variant is something else: 'sorry, the data is in the computer over there, and we've intentionally locked ourselves out of the computer.'"[127] This adds a certain ambiguity to CALEA's requirement that a communications company only be required to assist if it "possesses the information necessary to decrypt the communication."[128] If the company in question[129] possessed the information, but has deliberately destroyed it when it destroyed the access cards, it seems more difficult to invoke the statute's protection.

At the same time, the Cloud Key Vault setup suggests a way to keep a secure form of access to user's data: what Tait dubs an "Access Key Vault."[130] As Tait explains, "Apple devices store user backup files inside an envelope only [Apple's Cloud Key Vault] can decrypt and uploads this sealed envelope to Apple's servers."[131] He proposes an Access Key Vault (AKV) system, which

> by contrast, could store the device's decryption key inside an envelope only the AKV can decrypt, and store this AKV-sealed envelope on the device itself. This way, to get the AKV envelope, someone would need to first seize a device, and then forensically recover the AKV envelope from it. Only the AKV would be able to decrypt the sealed envelope with its secret private key, and thus nobody would be able to get at the individual device's decryption key inside without first delivering the envelope to AKV technicians who would then feed the envelope into the AKV vault for decryption.[132]

Under this scheme, only one in possession of the device could even begin the decryption process. The additional safeguards of automatic, undeletable logging of decryption attempts, the fact that the AKV secret private key would never leave Apple's headquarters, and "splitting keys over multiple AKVs distributed over

---

[126] *Id.*

[127] *Id.*

[128] *See* Morrison, *supra* note 1, at 2062 (quoting 47 U.S.C. § 1002(b)(3) (2012)).

[129] Again, this provision of CALEA only applies to telecommunications carriers, but for the sake of argument, let's assume it did cover Apple.

[130] Tait, *supra* note 119.

[131] *Id.*

[132] *Id.*

multiple organizations" would further raise the cost and complications of hacking.[133] Compromising such a system, argues Tait, "would require a grand conspiracy of technicians going rogue at multiple different organizations or that multiple air-gapped computer networks be hacked to compromise the technicians directly,"[134] and would be "limited to the unauthorized decryption of a small number of individually targeted devices to which the plotters must already have forensic local physical access."[135]

"Perhaps this scheme does not meet the platonic ideal of 'secure,'" concludes Tait, "but describing the risk as 'high potential for catastrophic loss' seems to me an abuse of ordinary language."[136] It does seem plausible that a system of nested keys to unlock phones that are in the possession of the government does not pose the kinds of security risks on a massive scale like the ones the public has already suffered.[137]

C. How Congress Might Move Forward

There has been a flurry of bills proposed so far, most of which either ban or fully endorse encryption. For example, the Secure Data Act of 2015 would "prohibit Federal agencies from mandating the deployment of vulnerabilities in data security technologies."[138] This bill would prohibit the government from "mandat[ing] that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency."[139] "Covered product[s]" include "any computer hardware, computer software, or electronic device that is made available to the general public."[140] This position is echoed in the language of the proposed ENCRYPT Act of 2016, which would prevent the government from interfering with any commercial encryption,[141]

---

[133] *Id.*

[134] *Id. But see* Hurwitz, *supra* note 5, at 414. He argues that the issue is not so much malefactors getting ahold of one of the escrowed keys, but "that it is simply very, very difficult to design a secure multi-party cryptosystem, and it is even more difficult to correctly implement that design." *Id.* Again, I will leave the technological feasibility of a split-key escrow system to the experts.

[135] Tait, *supra* note 119.

[136] *Id.*

[137] *See* Traylor, *supra* note 26, at 496–97 (listing some of the widespread data breaches of the past few years). And that was before over 140 million consumers had their personal information compromised in the Equifax breach. *See* Tara Siegel Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

[138] S. 135, 114th Cong. pmbl. (2015).

[139] *Id.* § 2(a).

[140] *Id.* § 2(c)(2).

[141] Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016, H.R. 4528, 114th Cong. § 2(a)(1)(A) (2016) (providing that no state or subdivision

and opposed by the Compliance with Court Orders Act of 2016, which would force companies to "provide such technical assistance as is necessary" to produce data "in an intelligible format."[142]

In June 2016, the House Committee on Homeland Security issued a report on the encryption debate, concluding that what was needed was a National Commission on Security and Technology Challenges constituted of "experts in the fields of commercial technology, computer science and cryptology, privacy and civil liberties, law enforcement, intelligence, and global economics."[143] This would allow a more nuanced balancing of interests. As the House Committee noted, the debate is not really about "privacy versus security" so much as it is between one type of security and another—the security of our data and infrastructure versus our physical public safety.[144]

It could be that the facts are as the privacy advocates say, and that the game of regulating technological assistance is not worth the candle. Ultimately, the issues of necessity, futility and security raise empirical questions that are best resolved by experts, and a commission or series of public hearings could do that job.

---

of a state may prohibit the use of encryption or compel any entity to "design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency or instrumentality of a State . . . or the United States").

[142] S.__, 114th Cong. § 3(a)(1)(B) (Discussion Draft 2016), https://www.eff.org/document/burr-feinstein-encryption-bill-discussion-draft [https://perma.cc/D9DS-89PS].

[143] STAFF OF H. HOMELAND SEC. COMM., 114TH CONG., GOING DARK, GOING FORWARD: A PRIMER ON THE ENCRYPTION DEBATE 4 (2016), https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf [https://perma.cc/S6YJ-HY4J]. A similar idea was suggested by former FBI Director James Comey, who called for "an adult conversation" on encryption. *See* Eric Tucker, *Comey: FBI Wants 'Adult Conversation' on Device Encryption*, AP (Aug. 31, 2016), http://bigstory.ap.org/article/7d57f5763f74b6ca4cd3436fbebf160/comey-fbi-wants-adult-conversation-device-encryption [https://perma.cc/DCW6-5N2S]. This prompted some mockery from the tech sector. *See, e.g.*, Mike Masnick, *James Comey Claims He Wants an 'Adult Conversation' About Encryption; Apparently 'Adults' Ignore Experts*, TECHDIRT (Aug. 31, 2016, 9:38 AM), https://www.techdirt.com/articles/20160831/00094935397/james-comey-claims-he-wants-adult-conversation-about-encryption-apparently-adults-ignore-experts.html [https://perma.cc/K5F2-G3L9] (describing Comey's call as "not just insulting, but counterproductive").

[144] *See* STAFF OF H. HOMELAND SEC. COMM., *supra* note 143, at 6. This is not to say that cellphone searches are limited to terrorism investigations, as they are also implicated in many other crimes, including kidnapping and human trafficking. *See* Vance, Jr. et al., *supra* note 16. There have also been a handful of murders where clues to the perpetrators' identity might have been found in locked smartphones. *See* Jacobsen, *supra* note 20, at 570–71 (citing the murders of Brittney Mills in April 2015 and Ray C. Owens in June 2015, and the possible murder of George Mitego in July 2015); *see also* Vance, Jr. et al., *supra* note 16. And the losses aren't just for prosecutors, as smartphone evidence has been used in exonerating innocent people as well. *See* Jacobsen, *supra* note 20, at 577–78.

III. WHAT SHOULD A DUTY TO ASSIST MEAN?

Let's say that the evidence points to the fact that the government is not entirely going dark, or that the evidence is inconclusive. We face the following situation: Apple, and companies like it, cannot comply with requests to help execute warrants because they have created a system where compliance is impossible. If there is a duty to assist, whether it is conceived of as a negative duty or a positive obligation, does that technological choice violate any such duty?

A. The Duty to Assist

"It is the duty and the right . . . of every citizen," observed the Supreme Court in 1895, "to assist in prosecuting, and in securing the punishment of, any breach of the peace of the United States."[145] The duty to assist the government in enforcing the law has deep common-law roots, as one state court explained: "The basic concept that every citizen can be compelled to assist in the pursuit or apprehension of suspected criminals has ancient Saxon origins, predating the Norman Conquest."[146]

Chief Judge Cardozo traced the obligation to help law enforcement "back to the [early] days of the hue and cry" in the thirteenth century.[147] This was a practice which obligated "[a]ll true men" to participate in the work of apprehending those charged with breaking the law.[148] Indeed, those who failed to do so, or did not keep adequate weaponry for the purpose,[149] were themselves liable to be prosecuted.[150] These

---

[145] *In re* Quarles, 158 U.S. 532, 535 (1895). The Court added: "It is the right, as well as the duty, of every citizen, when called upon by the proper officer, to act as part of the *posse comitatus* in upholding the laws of his country." *Id.* The *posse comitatus* "has been defined as the power or force of the county, consisting of the entire population of the county over the age of 15, which a sheriff may summon to his assistance in certain cases, such as keeping the peace, pursuing and arresting felons, etc." Williams v. State, 490 S.W.2d 117, 120 (Ark. 1973) (citing BLACK'S LAW DICTIONARY 1324 (4th ed. 1968)). "Refusal to render the aid sought by the sheriff was an offense punishable by fine and imprisonment." *Id.* (citations omitted).

[146] State v. Floyd, 584 A.2d 1157, 1166 (Conn. 1991).

[147] Babington v. Yellow Taxi Corp., 164 N.E. 726, 727 (N.Y. 1928).

[148] *See id.* ("'The main rule we think to be this,' say the historians of our early law (Pollock & Maitland, History of English Law, vol. 2, p. 580) 'that felons ought to be summarily arrested and put in gaol. All true men ought to take part in this work and are punishable if they neglect it.' *Cf.* Holdsworth, History of English Law, vol. 1, p. 294; vol. 3, p. 599; vol. 4, p. 521; Coyles v. Hurtin, 10 Johns. 85."). The *Babington* court further explained, "The law did not limit itself to imposing upon the manhood of the country a duty to pursue. To make pursuit effective, there were statutes in those early days whereby a man was subject to a duty to provide himself with instruments sufficient for the task." *Id.*

[149] Chief Judge Cardozo cited, as an example, the Statute of Winchester from 1285, which required that every man with sufficient property keep "an Hauberk [a Breastplate] of Iron, a Sword, a Knife, and an Horse." *Id.* (alteration in original).

[150] *See id.* ("We may be sure that the man who failed to use his horse, and who would only go afoot, would have had to answer to the king." (citations omitted)); *see also Williams*,

obligations persisted up to colonial times. The Colony of Massachusetts statutorily required citizens to "diligently pursue[ ]" the "Hue [and] cries,"[151] and provided that, if "any shal wilfully, obstinately or contemptuously refuse or neglect to assist any Constable . . . he shall pay to the use of the Country fourty shillings."[152] In the modern(ish)-day equivalent that Cardozo was considering, a police officer had jumped on the running board of a taxi, and ordered the driver to chase another car.[153] During the ensuing chase, the taxi driver was killed and the taxi company opposed paying Workmen's Compensation on the basis he was not in the performance of his duties at the time of the crash.[154] In rebuffing the taxi company, Cardozo was unequivocal: "[T]he citizenry may be called upon to enforce the justice of the state, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand."[155]

Moreover, he was clear that the duty also extended to corporate citizens: "The incorporeal being, the Yellow Taxi Corporation, would have been bound to respond in that spirit to the summons of the officer if it had been sitting in the driver's seat."[156]

Justice White, in his opinion in *New York Telephone*, recognized that similarly, "citizens have a duty to assist in enforcement of the laws."[157] There remain numerous state laws on the books criminalizing a failure or refusal to help law enforcement.[158] If the basis of these laws is still valid, then the demands on telephone

---

490 S.W.2d at 120 ("The criminal nature of refusal to aid an officer in the execution of his duties was recognized in Regina v. Brown, 41 Eng. Common Law Reports 175 (1841)."); Blue, *supra* note 15, at 1480–81 (noting that "if a malefactor was not caught by the hue and cry, a financial penalty would be levied on the entire township" (citing 2 HENRY DE BRACTON, ON THE LAWS AND CUSTOMS OF ENGLAND 350 (Samuel E. Thorne trans., 1968))). As the *Williams* court described it, in *Brown*, a constable came upon an illegal prize fight and sought to arrest the participants, enlisting the help of Brown. *Williams*, 490 S.W.2d at 120. The English court held that "one duly called upon to render such assistance was not excused except for physical impossibility or lawful excuse." *Id.* This rule then migrated the United States, where "the practice has been utilized in law enforcement throughout the history of this country." *Id.* at 120–21.

[151] Blue, *supra* note 15, at 1481 (citation omitted).

[152] THE BOOK OF THE GENERAL LAUUES AND LIBERTYES CONCERNING THE INHABITANTS OF THE MASSACHUSETS 13 (Cambridge, 1648).

[153] *See Babington*, 164 N.E. at 726.

[154] *Id.*

[155] *Id.* at 727.

[156] *Id.*

[157] United States v. N.Y. Tel. Co., 434 U.S. 159, 176 n.24 (1977).

[158] Blue notes that "[m]ost states statutorily authorize police officers to command bystanders to assist them in their law enforcement duties," and that many of those states "make a failure to obey such a command a criminal offense." Blue, *supra* note 15, at 1475–76; *see, e.g.*, ALA. CODE § 13A-10-5 (2017) (criminalizing refusal to aid police officer); CAL. PENAL CODE § 150 (West 2017) (same); COLO. REV. STAT. § 18-8-107 (2017); CONN. GEN. STAT. § 53a-167b (2017); DEL. CODE ANN. tit. 11, § 1241 (2017); FLA. STAT. § 843.06 (2017); N.Y. PENAL LAW § 195.10 (McKinney 2017); TEX. CODE CRIM. PROC. ANN. art. 2.15 (West 2017);

or information service companies could be thought of as a duty of citizenship. In that light, the government could prevent private citizens and companies from actively frustrating law enforcement investigations.

B. What Do We Do About Warrants?

The Supreme Court in *Katz v. United States*[159] famously observed that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[160] But what about a warrant without a search? If the "going dark" debate presents an empirical question, how much we should respect warrants raises a question of social ordering. It is not self-evident that private actors—in particular, commercial entities that profit by marketing themselves as champions of privacy—should be able to determine unilaterally that a certain class of information should be beyond the reach of law enforcement. Even if we accept the "Golden Age of Surveillance" premise, there is arguably something of value lost if certain types of warrants become meaningless.

Fourth Amendment jurisprudence is based in large part on deterring unlawful police conduct, and requiring a warrant is supposed to enhance police compliance with the law. There may be nothing magical about a search warrant,[161] but it is a manifestation of a social compact: government agents have the right to conduct reasonable searches and seizures, but the deal is that they cannot do so unless they get a warrant. (This statement is highly qualified, since almost no searches actually require warrants, but bear with me.) If they get a warrant based on probable cause,[162] they can search, as long as the search is reasonable. But if the warrants they obtain are pointless, this could conceivably undermine police respect for the process.[163] And it is rarely a good idea to encourage law enforcement to engage in self-help.

This is not to say that a search warrant or other court order, even one validly issued and based upon probable cause, provides absolute authorization to search. If there are circumstances that make the search unreasonable, even if it has been sanctioned by a judicial officer, the police cannot search.[164] For example, in *Winston v. Lee*,[165]

VT. STAT. ANN. tit. 24, § 301 (2017); VA. CODE ANN. § 18.2-463 (2017). Blue notes, however, "that these laws are not widely used." Blue, *supra* note 15, at 1476.

[159] 389 U.S. 347 (1967).

[160] *Id.* at 357 (citation omitted).

[161] *See* William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 VA. L. REV. 881, 883 (1991) (noting "the lack of any working theory of what warrants are supposed to accomplish"); *see also* Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609 (2012).

[162] Some types of searches, like wiretaps, statutorily require a showing of necessity as well, making Title III orders something like "super" warrants. *See* Kerr, *supra* note 47, at 1232.

[163] *See* Stuntz, *supra* note 161, at 909.

[164] *See* Winston v. Lee, 470 U.S. 753, 760 (1985).

[165] 470 U.S. 753 (1985).

the Supreme Court did not allow the police to "search" for a bullet in the chest of a robbery suspect.[166] Despite the fact that the police had probable cause and a court order, the Court found the search would be unreasonable because the extent of the intrusion, surgery under general anesthetic, was not outweighed by a "compelling need" on the part of the government.[167]

Once the government obtains a valid warrant based upon probable cause, wrote Justice Brennan, "it is ordinarily justifiable for the community to demand that the individual give up some part of his interest in privacy and security to advance the community's vital interests in law enforcement; such a search is generally 'reasonable' in the Amendment's terms."[168] But "compelled surgical intrusion into an individual's body for evidence," was not an ordinary search because it "implicate[d] expectations of privacy and security of such magnitude that the intrusion may be 'unreasonable' even if likely to produce evidence of a crime."[169] The Court therefore weighed the magnitude of the intrusion (surgery with a non-negligible risk of complications) against the community's need for the evidence.[170] Because the government had other sources of evidence, including eyewitness identification by the victim, the search was unreasonable.[171]

C. Reconstructing an Inviolable Zone of Privacy

One way of thinking about Apple's position is that making them assist in the execution of searches (which would entail breaking their own encryption, building backdoors, or what have you), is simply not reasonable.[172] In other words, the interference with the company's business or beliefs could be as damaging as the intrusion on the bodily integrity and dignitary concerns of a suspect.[173]

---

[166] *Id.* at 766. This was similar to the conclusion of the Indiana Supreme Court a decade earlier. *See* Adams v. State, 299 N.E.2d 834, 837 (Ind. 1973) (holding that, even with a valid search warrant, subjecting a robbery suspect to an operation to remove a bullet was unreasonable).

[167] *Winston*, 470 U.S. at 766.

[168] *Id.* at 759.

[169] *Id.*

[170] *See id.* at 763.

[171] *See id.* at 765.

[172] *Cf.* State v. Floyd, 584 A.2d 1157, 1159 (Conn. 1991) (holding that a statute criminalizing a failure to assist a police officer in effecting an arrest could only be applied if such assistance was both demonstrably necessary and "reasonable under all the circumstances").

[173] And Apple is not even the target of the search, but a third party innocent of wrongdoing. That said, Fourth Amendment law has not been overly solicitous of third parties in the past, as demonstrated by *United States v. Payner*, 447 U.S. 727 (1980). In a ruse right out of a spy movie, an IRS informant lured an unsuspecting bank manager out to dinner, making sure his briefcase remained at her apartment. *Payner*, 447 U.S. at 730. While a lookout team kept watch at the restaurant, another informant let himself into the apartment with a key supplied previously, stole the briefcase, and delivered it to IRS agents, who copied 400 pages

Ultimately, not to regulate encryption represents a decision to put a certain class of information—the kind that can be found on an individual's phone—beyond law enforcement reach. We could make the determination that this is the correct approach. But if companies are going to have the power unilaterally to exempt an entire class of information from searches, there should be adequate justification. One basis would be the unusually intimate and comprehensive trove of information to be found on people's phones. As Donald Dripps noted, there are "legitimate textual and historical grounds for treating 'papers' and their modern counterparts with more respect than other 'effects.'"[174]

One hundred and thirty years ago, in *Boyd v. United States*,[175] the Court intimated that there should be areas completely free from government surveillance. In *Boyd*, the Court invalidated an 1874 Customs Act that provided individuals subject to civil forfeiture with a choice: produce requested documents or have the allegations against them taken as confessed.[176] Upholding the Act, reasoned Justice Bradley, would sanction a "forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods."[177] This violated both the Fourth and Fifth Amendments, he wrote, because there was no substantial difference between "the seizure of a man's private books and papers to be used in evidence against him" and "compelling him to be a witness against himself."[178] Effectively, the "intimate relation" between the two amendments meant that "search and seizure of books and papers may be 'unreasonable' even if conducted pursuant to a court order."[179]

Boyd's vision of privacy was reaffirmed in *Gouled v. United States*,[180] which considered an ordinary search conducted pursuant to a valid search warrant. A warrant,

---

of documents, replacing it before the pair returned from dinner. *Id.* While the Court was aghast at the IRS's tactics, it had nothing to say about the inconvenience and indignity suffered by the bank manager. *See id.* at 734.

[174] Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 53 (2013). Dripps notes that statutory authority did not even exist for seizing private papers until 1863, when Congress passed "An Act to [P]revent and [P]unish Frauds upon the Revenue." *Id.* at 87.

[175] 116 U.S. 616 (1886).

[176] *See id.* at 620 ("[I]f [an individual, upon receiving a motion to produce] shall fail or refuse to produce such book, invoice, or paper in obedience to such notice, the allegations stated in the said motion shall be taken as confessed . . . ." (quoting Section 5 Act of June 22, 1874)).

[177] *Id.* at 630. Although *Boyd* was a civil case, the Court considered the proceedings to be "in their nature criminal." *Id.* at 634.

[178] *Id.* at 633. "In this regard the Fourth and Fifth Amendments run almost into each other." *Id.* at 630. *See generally* Note, *The Life and Times of* Boyd v. United States *(1886–1976)*, 76 MICH. L. REV. 184 (1977) [hereinafter *Life and Times*].

[179] *Life and Times*, *supra* note 178, at 184.

[180] 255 U.S. 298 (1921).

wrote the Court, "may not be used as a means of gaining access to a man's house or office and papers solely for the purpose of making search to secure evidence to be used against him in a criminal or penal proceeding."[181] In other words, the government had to have some property interest in the items to be seized (or demonstrate that possession of the items by the suspect was unlawful), or it could not seize them at all.[182] Papers of "mere evidential value" were beyond the scope of a lawful warrant—the so-called "mere evidence rule."[183]

But the decisions following *Boyd* and *Gouled* began to "reduce[ ] the obstacles to governmental seizure of an individual's property," and "narrow[ ] his effective zone of privacy."[184] The mere evidence rule was officially laid to rest in *Warden v. Hayden*,[185] and by the time the Court issued its decision in *Katz v. United States*,[186] the Court no longer seemed to believe that any area, of itself, was immune to search, so long as a warrant was obtained and the search was conducted in a reasonable manner.[187]

Still, there is an aura that surrounds private papers, and by extension, most of the information on computers and mobile devices, that could support different treatment.

Maybe history supports Apple. But if so, that is a decision to be made in a public forum, by the courts or the legislature, in a reasoned fashion.

---

[181] *Id.* at 309.

[182] *See id.* The Court did note that "[t]here is no special sanctity in papers, as distinguished from other forms of property, to render them immune from search and seizure," so long as they were adequately described in the warrant and belonged to a class of documents that could be seized, such as "[s]tolen or forged papers" or "lottery tickets." *Id.*

[183] *See id.* at 310; *see also Life and Times*, *supra* note 178, at 191.

[184] *Life and Times*, *supra* note 178, at 193. This idea found its most eloquent expression in Justice Brandeis's dissent in *Olmstead v. United States*, 277 U.S. 438 (1928). The *Olmstead* Court had upheld the right of the FBI to tap Olmstead's phone without a warrant, because doing so did not invade his property rights. *See id.* at 466 (relying on the fact that "the [telephone] wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment"). Justice Brandeis's dissent famously argued that the Fourth Amendment's point was not to enforce property law but to protect a "right to be let alone"—in other words, not that all searches needed a warrant, but that some searches should not happen at all:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.

Id. at 478 (Brandeis, J., dissenting).

[185] 387 U.S. 294 (1967).

[186] 389 U.S. 347 (1967).

[187] As now-professor Krauss put it in his student note, "[n]o zone of privacy now exists that the government cannot enter." *Life and Times*, *supra* note 178, at 211. *See generally* Stanton David Krauss, http://webspace.quinnipiac.edu/Krauss/RESUME%20for%20web%20page.pdf [https://perma.cc/XS25-SG5B] (providing Prof. Krauss's résumé, in which he is listed as the author of the unsigned student note, *Life and Times*, *supra* note 178).

CONCLUSION

We end up where we began, with our original question: What assistance do private actors owe law enforcement? Apart from antiquated laws that require assistance when the police are pursuing a suspect, the law rarely requires companies to take positive action. Asking companies to conform their design and innovation strategies to government blueprints does seem to interfere with their autonomy. The wrinkle here is that Apple has specifically designed a system that it cannot itself access—it built a key, locked itself out, then destroyed the key.

In an ideal world, there would be a Congressional solution, based on a factual balancing of the different interests. As the situation stands, the tech sector and the government can only look forward to more litigation, more conflict, and more uncertainty. To have some clarity in this area would be good. Having a coherent principle to justify the solution would be even better.