Boston College Law Review

Volume 57 | Issue 4 Article 9

9-28-2016

A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act

John L. Potapchuk
Boston College Law School, john.potapchuk@bc.edu

Recommended Citation

John L. Potapchuk, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act*, 57 B.C.L. Rev. 1403 (2016), http://lawdigitalcommons.bc.edu/bclr/vol57/iss4/9

A SECOND BITE AT THE APPLE: FEDERAL COURTS' AUTHORITY TO COMPEL TECHNICAL ASSISTANCE TO GOVERNMENT AGENTS IN ACCESSING ENCRYPTED SMARTPHONE DATA UNDER THE ALL WRITS ACT

Abstract: On February 29, 2016, in *In re Order Requiring Apple, Inc. Assist in Execution of Search Warrant* (*"In re Apple, Inc."*) the U.S. District Court for the Eastern District of New York held that the All Writs Act did not provide the legal authority to require Apple Inc. to bypass the encrypted lock-screen passcode of an iPhone for the federal government in order to execute a search warrant. Accordingly, the decision, which was the first of its kind, stripped the government of an investigative tool upon which it had routinely relied since as early as 2008. In *In re Apple, Inc.*, after years of acquiescence to such orders, Apple mounted its first challenge to the propriety of the All Writs Act and courts' authority to compel the company to bypass its own encryption for the government. This position followed from Apple's most recent efforts to provide tighter mobile security for its customers with the rollout of iOS 8 in October 2014, which offered more extensive full-disk encryption by default—so extensive, Apple claimed, that its previous assistance to the government is no longer technologically feasible. As a result of the newly enhanced encryption law enforcement officials across the country have encountered hundreds of lawfully searchable phones with no means of executing searches. This Note provides a discussion of the underlying legal implications surrounding the heated public debate that has emerged in the wake of *In re Apple, Inc.* and other similar cases as well as the practical challenges enhanced data encryption creates for law enforcement officials. Particularly, it focuses on the propriety of decryption assistance orders that have been issued under the All Writs Act. It argues that the decision in *In re Apple, Inc.* was incorrect, and that the All Writs Act does in fact confer authority to federal courts to compel third-party assistance in certain situations. It concludes by offering an expansion of the Communication Assistance to Law Enforcement Act as one potential solution to the threat that impenetrable device encryption poses to the functioning of the American criminal justice system.

INTRODUCTION

If you own a smartphone with a lock-screen passcode, you most likely use encryption or at least have the option to turn it on.[1] The extent to which that encryption is secure depends on a myriad of factors, most notably the device and its operating system.[2] Full-disk encryption, once an underappreciated and underutilized security feature available for smartphones, has proliferated in recent years.[3] Its increasingly widespread use as a default feature on newer devices is flooding the market with phones designed to be impenetrable when locked.[4] Since October 2014, versions of Apple's iOS and Google's Android, which collectively comprise over ninety-six percent of the worldwide operating-system market share for smartphones, have supported encryption capabilities originally believed to be impossible to circumvent without the owner's passcode.[5]

[1] *See, e.g.*, Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand Over Passwords*, 30 BERKELEY TECH. L.J. 1, 7–8 (2015) (noting that the increased societal reliance on mobile computing and digital storage has sparked demand for more sophisticated encryption technology); Matt Appuzzo et al., *Apple and Other Tech Companies Tangle with U.S. Over Data Access*, N.Y. TIMES (Sept. 7, 2015), http://nyti.ms/1UCWAgf [https://perma.cc/XG4N-TNQ6] (discussing the increased demand for built-in cellphone encryption modes available for encrypting digital communication and data stored on cellphones); Andrew Cunningham, *Phone and Laptop Encryption Guide: Protect Your Stuff and Yourself*, ARS TECHNICA (Aug. 23, 2015, 1:00 PM), http://arstechnica.com/gadgets/2015/08/phone-and-laptop-encryption-guide-protect-your-stuff-and-yourself/1/ [https://perma.cc/C75P-BQN8] (discussing methods available for encrypting digital storage on various smartphones offered by Google, Microsoft, and Apple).

[2] *See* Cunningham, *supra* note 1 (discussing the effectiveness of comparable full-disk encryption operating systems offered by Google, Microsoft, and Apple as of August 2015); Ryan Radia, *Why You Should Always Encrypt Your Smartphone*, ARS TECHNICA (Jan. 16, 2011, 11:00 PM), http://arstechnica.com/gadgets/2011/01/why-you-should-always-encrypt-your-smartphone [https://perma.cc/WBF4-BNJA].

[3] *See* Cunningham, *supra* note 1 (noting the prevalence of mobile operating systems that support full-disk encryption); Radia, *supra* note 2. Full-disk encryption is largely considered one of the most secure cryptosystems available for data stored on electronic devices. *See* Radia, *supra* note 2. Available in the form of both hardware and software, full-disk encryption converts everything on the hard drive, including the operating system, into an unreadable form until the phone's password is entered. *See* Wilson, *supra* note 1, at 7–8.

[4] *See* Appuzzo et al., *supra* note 1 (discussing new encryption on Apple and Android phones); Joseph Menn et al., *Apple's War with the FBI Could Speed up the Developments of Government-Proof Tech*, BUS. INSIDER (Feb. 24, 2016, 7:02 AM), http://www.businessinsider.com/r-apples-fight-with-us-could-speed-development-of-government-proof-devices-2016-2 [https://perma.cc/YLT7-XJ67] (discussing the emerging market for smartphones specifically designed to thwart snooping governments, criminals, and corporate rivals, such as BlackPhone, RedPhone, and the BlackBerry Priv).

[5] *See* Cat Zakrzewski, *Encrypted Smartphones Challenge Investigators*, WALL STREET J. (Oct. 12, 2015, 7:36 PM), http://www.wsj.com/articles/encrypted-smartphones-challenge-investigators-1444692995 [https://perma.cc/U543-EJC4]; Press Release, Gartner, Gartner Says Worldwide Smartphone Sales Grew 9.7 Percent in Fourth Quarter of 2015 (Feb. 18, 2016), http://www.gartner.com/newsroom/id/3215217 [https://perma.cc/L9JR-8G43].

The new enhancements in device encryption are creating significant problems for law enforcement personnel, however, who are increasingly obtaining warrants to search the smartphones of criminal suspects and homicide victims with no means of executing those searches.[6] In the past, Apple had regularly assisted law enforcement officials in bypassing the passcodes of seized phones in response to a valid court order and search warrant.[7] That assistance, Apple claims, is no longer an option with updated phones because the newer encryption is designed to make it impossible for anyone, even company technicians, to access a locked phone without the passcode.[8] Additional security features, such as automatic data-wiping protocols, may nullify many alternative methods of hacking into phones.[9]

Collectively, these newer impediments effecting law enforcement's ability to access stored data represent the most recent installment in a larger issue colloquially referred to as "Going Dark."[10] Generally, the term refers to the evolving gap between the government's authority to conduct criminal investigations and the ability to exercise that authority in light of technological advancements.[11] Enhanced encryption has reignited a simmering debate

[6] *See* KRISTIN FINKLEA, CONG. RESEARCH SERV., R44187, ENCRYPTION AND EVOLVING TECHNOLOGY: IMPLICATIONS FOR U.S. LAW ENFORCEMENT INVESTIGATIONS 6, 7 (2016); Zakrzewski, *supra* note 5 (discussing investigators from across the country encountering problems).

[7] *See* FINKLEA, *supra* note 6, at 6; Jason M. Weinstein et al., *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era*, 52 AM. CRIM. L. REV. 729, 744 (2015).

[8] *See* FINKLEA, *supra* note 6, at 5–7; Daisuke Wakabayashi, *Apple's Evolution into a Privacy Hard-Liner*, WALL STREET J. (Feb. 23, 2016, 8:59 PM), http://www.wsj.com/articles/apples-evolution-into-a-privacy-hard-liner-1456277659?mod=pls_whats_news_us_business_f [https://perma.cc/5AE2-M74C].

[9] *See* FINKLEA, *supra* note 6, at 8; Orin Kerr, Opinion, *Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case (Part 1)*, WALL STREET J. (Feb. 18, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/18/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-1 [https://perma.cc/L7A8-4CWS]; *see infra* note 45 and accompanying text (discussing the auto-erase function available on iPhones and the protection that function provides against brute-force forensic techniques).

[10] *E.g.*, FINKLEA, *supra* note 6, at 8–9 (discussing the evolution of the "going dark debate," which originally centered on law enforcement's ability to intercept real-time communication, but has since extended beyond the realm of traditional and cellular telephone communications due to technological innovations in other areas, such as enhanced data encryption); Geoffrey S. Corn, *Averting the Inherent Dangers of "Going Dark": Why Congress Must Require a Locked Front Door to Encrypted Data*, 72 WASH. & LEE L. REV. 1433, 1433–44 (2015) (discussing the same).

[11] *See* FINKLEA, *supra* note 6, at 8–9; James B. Comey, Dir., FBI, Remarks at Brookings Institution (Oct. 16, 2014), http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/7JTL-BJRK]. The Going Dark issue has become two-pronged, and currently pertains to both real-time communication, or "data in motion;" as well as stored data, or "data at rest." *See* FINKLEA, *supra* note 6, at 9; Comey, *supra* (discussing the "two overlapping challenges" pertaining to the Going Dark issue). Each type of data is protected by a different form of an encryption: for example, data in motion tends to be protected by "end-to-end encryption," whereas data at rest can be protected by the full-disk en-

between government officials and technology executives regarding the proper balance between data security and effective law enforcement.[12] Moreover, recent court proceedings have drawn particular attention to the government's practice of obtaining uncontested court orders requiring Apple to provide technical assistance in accessing locked devices, which it has relied upon for several years.[13] In October 2015, in *In re Order Requiring Apple, Inc. Assist in Execution of Search Warrant* ("*In re Apple, Inc.*"), before U.S. Magistrate Judge James Orenstein in the U.S. District Court for the Eastern District of New York, Apple asserted its first challenge to such an order-application.[14] Apple argued that it no longer conceded that the All Writs Act grants the authority to federal courts to order it to provide assistance to the government.[15] Judge Orenstein agreed, and entered a decision

cryption ("FDE"). Appuzo et al, *supra* note 1; David G. Ries & John W. Simek, *Encryption Made Simple for Lawyers*, GP SOLO, Nov.–Dec. 2012, at 18, 20.

[12] *E.g.*, FINKLEA, *supra* note 6, at 8–9; Corn, *supra* note 10, at 1433–34.

[13] *See* Joe Palazzolo & Devlin Barrett, *Roots of Apple-FBI Standoff Reach Back to 2008 Case*, WALL STREET J. (Apr. 7, 2016, 2:00 PM), http://www.wsj.com/articles/roots-of-apple-fbi-standoff-reach-back-to-2008-case-1460052008 [https://perma.cc/H4MQ-NY54].

[14] *See* Transcript of Argument Before the Honorable James Orenstein U.S. Magistrate Judge at 55–56, *In re* Order Requiring Apple, Inc. Assist in Execution of Search Warrant, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-01902) [*hereinafter In re Apple, Inc.*, Transcript of Oct. 26, 2015]. Judge Orenstein is one of several magistrate judges that has been implicated in the "magistrates' revolt," which has been used to refer to a string of denials of questionable federal government surveillance applications over the past decade. *See* Nicole Hong, *Apple Encryption Fight Pushes Magistrate Judges into New Legal Frontier*, WALL STREET J. (Mar. 1, 2016, 1:45 PM), http://www.wsj.com/articles/apple-encryption-fight-pushes-magistrate-judges-into-new-legal-frontier-1456857948 [https://perma.cc/Q64H-32VH].

[15] *See In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 61–62; *see also* 28 U.S.C. § 1651(a) (2012) (the All Writs Act). Between October 2015 and February 2016, at least nine additional orders were issued by federal courts across the country directing Apple to assist the government in bypassing the passcodes of iPhones running on a variety of iOS versions, all pursuant to the All Writs Act. *See In re* Order Requiring Apple, Inc. Assist in Execution of Search Warrant (*In re Apple, Inc.*), 149 F. Supp. 3d 341, 349 (E.D.N.Y. 2016). Notably, one such order went as far as directing Apple to *create* and load Apple-signed software onto the phone of Syed Rizwan Farook, one of the San Bernardino gunmen, to disable the phone's auto-erase function to enable the government to access the phone's data with the help of forensic tools. *See In re* Apple iPhone Seized During the Execution of Search Warrant on Black Lexus IS300 (*The San Bernardino Shooter Case*), No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016); Devlin Barrett, *San Bernardino iPhone Hack Doesn't Work on Newer Models, FBI Says*, WALL STREET J. (Apr. 7, 2016, 4:45 PM), http://www.wsj.com/articles/san-bernardino-iphone-hack-doesnt-work-on-newer-models-fbi-director-says-1460050154 [https://perma.cc/X2PD-EXEQ]. Specifically, the court noted that "technical assistance" may include providing the FBI with a Software Image File ("SIF"), signed by Apple, that can be loaded onto the phone to modify the iPhone's iOS using a mode traditionally used for device upgrades. *See The San Bernardino Shooter Case*, 2016 WL 618401, at *1. Furthermore, the court directed that the SIF be coded with a unique identifier so that the SIF will only load and execute on the target phone. *See id.* The government later withdrew its claim after purchasing a forensic tool from a private third party that allowed it to unlock the phone without Apple's assistance. *See* Barrett, *supra* note 15. James Comey later indi-

holding the All Writs Act as unavailable as a matter of law to direct third-party assistance in this context, which represents the first of its kind.[16] Although many believe that the issue will eventually be settled through legislation, the government's interim efforts to get into several locked phones has drawn much attention to the propriety of the All Writs Act and the federal courts' authority to command private assistance in order to effectuate a warrant.[17]

This Note will discuss the federal courts' authority to issue orders upon third parties to provide technical assistance to the government under the All Writs Act, and the related implications within the debate regarding cellphone encryption of data at rest.[18] Part I discusses the encryption of data at rest on cellphones, particularly the type of encryption used on iPhones, and further discusses some of the constitutional and statutory implications that arise when law enforcement officials wish to search a cellphone.[19] Part II discusses the All Writs Act particularly its application by the federal district courts to compel third-party assistance.[20] Part III discusses *In re Apple, Inc.*, in which Judge Orenstein denied the government's application for an order compelling Apple to provide technical assistance under the All Writs Act.[21] Part IV argues that the All Writs Act does authorize the court to order companies like Apple to provide technical assistance under certain circumstances, but that the ultimate solution to the encryption problem should come from Congress by expanding the Communication Assistance to Law Enforcement Act ("CALEA").[22]

cated that although the tool successfully opened the iPhone 5C at issue, it could not be used on newer iPhone models, such as the 5S or the 6. *See id.*

[16] *See In re Apple, Inc.*, 149 F. Supp. 3d at 346–47, 349; *In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 55, 62.

[17] *See* Corn, *supra* note 10, at 1444–46 (discussing potential solutions to Going Dark); Devlin Barrett & Daisuke Wakabayashi, *FBI Chief, Apple Lawyer Take Encryption Fight to Capitol Hill*, WALL STREET J. (Mar. 1, 2016, 6:43 PM), http://www.wsj.com/articles/amid-encryption-fight-attorney-general-urges-cooperation-1456830001?mod=trending_now_ [https://perma.cc/QU3M-6MWX] (quoting executive branch officials' congressional testimony regarding Going Dark and the government's proceedings against Apple); Hong, *supra* note 14 (discussing ongoing proceedings of March 2016). On February 29, 2016, a bill was introduced in the House of Representatives to establish a legislative advisory commission comprised of individuals from various fields to investigate the cellphone encryption issues and provide recommendations to Congress. *See* H.R. 4651, 114th Cong. (2016).

[18] *See infra* notes 23–222 and accompanying text.

[19] *See infra* notes 30–86 and accompanying text.

[20] *See infra* notes 92–142 and accompanying text.

[21] *See infra* notes 149–170 and accompanying text.

[22] *See infra* notes 181–222 and accompanying text.

I. ENCRYPTION, GOING DARK, AND THE CONSTITUTIONAL AND STATUTORY IMPLICATIONS OF SEARCHING A LOCKED SMARTPHONE

Although government officials have decried the problem of "Going Dark" for well over a decade, up until recently, such concerns were not necessarily focused on digital *data at rest*, contained on cellphones, but rather digital *data in motion*.[23] Accordingly, recent improvements in encryption protecting data at rest have brought a slew of new obstacles that law enforcement must now navigate throughout the course of otherwise routine investigations.[24] This Part discusses cellphone data encryption and the investigative impediments that it creates for law enforcement officials.[25] Section A of this Part provides a brief overview of data encryption and its use in smartphones.[26] Section B discusses the evolution of the data encryption on Apple's iOS operating systems for iPhones and the current capabilities of the encryption technology on iOS 8 and higher.[27] Section C provides a brief overview of the constitutional implications involved in governmental cellphone searches.[28] Finally, Section D discusses the potentially relevant federal statutes implicated in searching an encrypted cellphone and more background on the Going Dark debate.[29]

A. What Is Encryption?

Encryption is the transformation of a plaintext message, by some predesigned protocol, into an enciphered form, known as "ciphertext," in such a way that hides the substance of its content.[30] Similarly, decryption is the inverse process of recapturing the content of that message.[31] The "crypto-

[23] *See* Corn, *supra* note 10, at 1433–45.

[24] *See id.* at 1434–45.

[25] *See infra* notes 30–86 and accompanying text.

[26] *See infra* notes 30–36 and accompanying text.

[27] *See infra* notes 37–53 and accompanying text.

[28] *See infra* notes 54–65 and accompanying text.

[29] *See infra* notes 66–86 and accompanying text.

[30] *See* Benjamin Folkinshteyn, *A Witness Against Himself: A Case for Stronger Legal Protection of Encryption*, 30 SANTA CLARA HIGH TECH. L.J. 375, 378 (2014); Jeffrey L. Vagle, *Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance*, 90 IND. L.J. 101, 117 (2015).

[31] CZESŁAW KOŚCIELNY ET AL., MODERN CRYPTOGRAPHY PRIMER 1 (2013). "Protocol" is an operation that transforms the message into an unintelligible string of ciphertext, generally by applying some form of mathematical function. *See id.* at 37; Vagle, *supra* note 30, at 117. Together, the encryption and decryption algorithms form a "cipher," or "cryptosystem," with the goal of providing secret communication. *See* KOŚCIELNY ET AL., *supra*, at 3.

graphic key" is an additional input component known only to the designer and user, and its strength is crucial to a cipher's effectiveness.[32]

Today, encryption technology ("cryptography") is widely used by governments, businesses, and individuals throughout the world on a wide range of devices, increasingly including smartphones.[33] In terms of reliable and practical cryptography, one of the earliest types of encryption software available for stored data on smartphones was full-disk encryption ("FDE").[34] FDE functions by converting everything on a phone's hard drive, including the operating system, into unreadable ciphertext until the phone's password is entered.[35] Until recent years, few hardware-based FDE services were available for smartphones, but they have now become more widespread.[36]

B. An Apple Falls into the Darkness: Apple's Encryption and Going Dark

The encryption technology used on Apple's iPhones has evolved from fairly rudimentary to highly sophisticated and secure due to the steady implementation of increasingly better variations of FDE and remote wiping capabilities over the past decade.[37] Until the release of iOS 8 in October

[32] KOŚCIELNY ET AL., *supra* note 31, at 3. A key usually takes the form of a number, but can be a representation of any value, and its strength is critical because most algorithms and protocols are publicly known and can be analyzed by experts. *Id.*

[33] *E.g.*, Vagle, *supra* note 30, at 120–22. Today, modern encryption is available for smartphones in a variety forms: software, hardware, and built-in encryption in operating systems. *See id.* at 119; Ries & Simek, *supra* note 11, at 20. Encryption designed to protect data on hard drives can be further grouped into two general categories: "file-level encryption" and "disk-level encryption." Folkinshteyn, *supra* note 30, at 379; Ries & Simek, *supra* note 11, at 20.

[34] *See* Radia, *supra* note 2. In comparison, "end-to-end encryption" protects data in transit between users, such as email and message services. *See* Jon Czas, *Note: Business, Law, and Project Prism*, 12 GEO. J.L. & PUB. POL'Y 897, 898 & n.11 (2014). Real-time interception of communications protected by end-to-end encryption, such as phone calls and emails, which is provided by telecommunications carriers and broadband providers, is governed at the federal level by the Communication Assistance for Law Enforcement Act ("CALEA"). *See* Comey, *supra* note 11; *see also* 47 U.S.C. §§ 1001–10 (2012) (CALEA).

[35] *E.g.*, KAREN SCARFONE ET AL., GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES 3-1 (2007); Wilson, *supra* note 1, at 7–8. Full-disk encryption, or disk-level encryption, is distinguishable from file-level encryption in that it encrypts everything on a hard drive, rather than individual files. Folkinshteyn, *supra* note 30, at 379; Ries & Simek, *supra* note 11, at 20. File-level encryption, often offered as smartphone applications, has at times been considered to offer less security, because any data outside one of those files is not protected. *See* Radia, *supra* note 2.

[36] *See* Ries & Simek, *supra* note 11, at 21; Radia, *supra* note 2. On hardware-based systems, the cryptographic keys are stored on the hard drive instead of the computer's memory, which makes key recovery more difficult and curbs the risk of malware and other threats. *See* SCARFONE ET AL., *supra* note 35, at 3-2 to -3. Additionally, hard-ware based systems can only be managed locally, whereas software-based FDE can be centrally managed on a remote server. *See id.* at 3-2.

[37] See Jacqui Cheng, *Can Apple Give Police a Key to Your Encrypted iPhone Data? Ars Investigates*, ARS TECHNICA (Apr. 4, 2012), http://arstechnica.com/apple/2012/04/can-apple-give-police-a-key-to-your-encrypted-iphone-data-ars-investigates [https://perma.cc/SGU7-U7YZ]; Radia, *supra*

2014, Apple possessed the capabilities to bypass any iPhone's lock screen passcode and turn over certain data—SMS iMessages, MMS, photos, videos, contacts, call history, etc.—to authorities in response to a search warrant.[38] Alternatively, authorities possessed the ability in many cases to guess a phone's passcode using simple forensic tools.[39] As part of the iOS 8 rollout, Apple announced an update in its privacy policy, which claimed that under the new encryption system "it's not technically feasible" for the company to cooperate with government warrants for the extraction of personal data.[40] Like previous versions, iOS 8 is equipped with "Data Protection" software that encrypts individual applications/files using an encryption key, which is derived from an entanglement of the user-created password and an ID number, unique to each iPhone ("UID").[41] The encryption key is the product of running both the password and the UID through a key derivation function calibrated with an 80-millisecond iteration count, which makes each attempt at unlocking the device slower.[42] Apple estimates that a brute-force attack at trying all possible combinations of a six-character alphanumeric passcode may take up to 5½ years to complete, depending on the passcode's strength.[43] The principal difference between iOS 8 and previous versions is that under iOS 8, more data-sensitive applications receive that

note 2; David Schuetz, *A (Not So) Quick Primer on iOS Encryption*, DARTH-NULL.ORG (Oct. 6, 2014), http://www.darthnull.org/2014/10/06/ios-encryption [https://perma.cc/86PA-6EKT].

[38] *E.g.,* FINKLEA, *supra* note 6, at 6; Weinstein et al., *supra* note 7, at 744.

[39] *See* DINO A. DAI ZOVI, TRAIL OF BITS, APPLE IOS 4 SECURITY EVALUATION 25, 29 (2011). This technique of "guessing" all possible combinations is known as a "brute-force" attack, which normally involves a computer program that can attempt every possible combination of characters until it finds the correct one. *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 430–32 (2012).

[40] *E.g.,* FINKLEA, *supra* note 6, at 5.

[41] *See* APPLE, INC., IOS SECURITY-WHITEPAPER 9–11 (Oct. 2014); Matthew Green, *Is Apple Picking a Fight with the U.S. Government?*, SLATE (Sept. 23, 2014, 10:51 AM) [hereinafter Green, *Is Apple Picking a Fight?*], http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html [https://perma.cc/9Y9Z-M8NW]. The UID is stored in the hardware and very difficult to extract. *See* Matthew Green, *Why Can't Apple Decrypt Your Phone?*, CRYPTOGRAPHIC ENGINEERING BLOG (Oct. 4, 2014, 4:05 PM) [hereinafter Green, *Why Can't Apple Decrypt?*], http://blog.cryptographyengineering.com/2014/10/why-cant-apple-decrypt-your-iphone.html [https://perma.cc/D5GJ-J9TL]; *see also* APPLE, INC., *supra* note 41, at 11 ("The passcode is entangled with the device's UID . . . ."). According to Apple's October 2014 Security Guide: "No software or firmware can read them directly; they can only see the results of encryption or decryption operations performed using them. The UID is unique to each device and it's not recorded by Apple or any of its suppliers." APPLE, INC., *supra* note 41, at 9.

[42] *See* APPLE, INC., *supra* note 41, at 11; Green, *Is Apple Picking a Fight?*, *supra* note 41. On certain devices with an A7 or later A-series processor, a 5-second delay between failed unlocking attempts is also enforced to further prevent brute-force attacks. *See* APPLE, INC., *supra* note 41, at 11.

[43] *See* APPLE, INC., *supra* note 41, at 11; Green, *Is Apple Picking a Fight?*, *supra* note 41. By comparison, a similar feature on iOS 4, still allowed a four-digit passcode to be guessed in under 20 minutes. *See* DAI ZOVI, *supra* note 39, at 26–27, 29.

encryption by default, which Apple cannot extract by circumventing the passcode.[44]

Further protection can be enabled by activating a feature from the settings menu that will permanently wipe all of the data from a phone in the event a password is entered incorrectly ten consecutive times.[45] The data encryption keys for recent iPhones—5S, 6, 6 Plus, 6S, or 6S Plus—are now stored in a hardware-based encryption co-processor, known as the "Secure Enclave."[46] Apple claims that it does not possess the capability to break into an iPhone's Secure Enclave; but to do so, security experts have noted that a type of digital "skeleton key" would have to have been designed to which only the company has access, colloquially known as a "backdoor."[47] Backdoors in any cryptosystem raise serious security concerns, because it is difficult to ensure that the intended access point will not be discovered and exploited by hackers or foreign intelligence agencies.[48]

Google also initially reported in 2014 that the next version of its Android operating system, "Android 5.0 Lollipop," would support full-disk encryption by default.[49] These moves from the two tech-giants reflect the

[44] *See* Green, *Is Apple Picking a Fight?*, *supra* note 41; APPLE, INC., *supra* note 41, at 10 ("Key system apps, such as Messages, Mail, Calendar, Contacts, Photos, and Health data values use Data Protection by default, and third-party apps installed on iOS 7 or later receive this protection automatically."); *see also* Green, *Why Can't Apple Decrypt*, *supra* note 41 ("So to a large extent the 'new' feature Apple is touting in iOS 8 is simply that they're encrypting more data."). For example, photos and text messages were not previously encrypted under the passcode. *See* Green, *Why Can't Apple Decrypt*, *supra* note 41.

[45] *See* APPLE, INC., *supra* note 41, at 11. This function creates a significant protection against brute-force attacks, which have typically been used by law enforcement to unlock phones with the help of forensic tools. *See* Kerr, *supra* note 9. For example, the assistance sought from the FBI in the *The San Bernardino Shooter Case*, was an order that would direct Apple to develop a software update that could be uploaded to the targeted iPhone to disable this auto erase function. *See The San Bernardino Shooter Case*, 2016 WL 618401, at *1; Kerr, *supra* note 9.

[46] *See* APPLE, INC., *supra* note 41, at 6–7, 9; Green, *Is Apple Picking a Fight?*, *supra* note 41.

[47] *See* Green, *Is Apple Picking a Fight?*, *supra* note 41; *see also Privacy—Government Information Requests*, APPLE INC. [hereinafter *Apple Privacy—Gov't Info. Req.*], http://www.apple.com/privacy/government-information-requests [https://perma.cc/MN5P-L5ZA] ("For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."). As of March 7, 2016, Apple estimates that 95% of its devices are running on iOS 8 or higher. *See Support: App Store*, APPLE DEVELOPER, https://developer.apple.com/support/app-store/ [https://perma.cc/N8FV-4L33].

[48] *See* FINKLEA, *supra* note 6, at 10; Swire & Ahmad, *supra* note 39, at 432–33, 436; Ellen Nakashima, *Tech Giants Don't Want Obama to Give Police Access to Encrypted Phone Data*, WASH. POST (May 19, 2015), https://www.washingtonpost.com/world/national-security/tech-giants-urge-obama-to-resist-backdoors-into-encrypted-communications/2015/05/18/11781b4a-fd69-11e4-833c-a2de05b6b2a4_story.html [https://perma.cc/832V-5VQP].

[49] *See* Weinstein et al., *supra* note 7, at 745; Andrew Cunningham, *Google Quietly Backs Away from Encrypting New Lollipop Devices by Default [Updated]*, ARS TECHNICA (Mar. 2, 2015, 12:00 PM), http://arstechnica.com/gadgets/2015/03/google-quietly-backs-away-from-encrypting-new-lollipop-devices-by-default/ [https://perma.cc/H8BL-H3S7]. Although only a few devices

larger, and rather explosive trend among technology firms that have embraced tighter encryption in the wake of the Snowden revelations.[50] Although such efforts have been generally lauded by privacy advocates, many government officials have cautioned that such widespread encryption may make it impossible for police to execute search warrants on lawfully seized devices.[51] Federal and state law enforcement officials have repeatedly emphasized the danger in expressly marketing products that enable terrorists and domestic criminals to place themselves beyond the reach of the law.[52] The debate over Going Dark, which continues to play out before the federal judiciary and congressional committees, presents unique and profoundly important questions regarding the appropriate balance between private and public security under the Fourth Amendment.[53]

C. Federal Constitutional Implications Involved in Searching a Smartphone

The Fourth Amendment of the U.S. Constitution guarantees people the right to be free from certain kinds of governmental intrusion, namely unreasonable searches and seizures.[54] In the context of a search, this protection

running Lollipop have actually encrypted by default, Google has indicated that FDE will be a requirement in future Android versions, and that performance issues have hindered its implementation thus far. *See* Cunningham, *supra*.

[50] *See*, Joris V.J. van Hoboken & Ira S. Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 ME. L. REV. 487, 508–10 (2014) (discussing the reactions and industrial solutions to consumer distrust in the wake of the Snowden revelations, specifically in the context of Cloud computing and flows between data centers); Menn et al., *supra* note 4 (discussing heavily secured smartphones and the market trends among technology firms, such as Google, Apple, and Facebook Inc., who have been incorporating bolstered encryption technologies into their products and services). The Snowden revelations refer to a number of released documents, beginning in June 2013, by Edward Snowden, former U.S. National Security Agency ("NSA") contractor, which revealed that the NSA had been collecting mass quantities of customer records from cloud computing platforms, U.S. wireless carriers, and several internet service providers under the authority of Section 215 of the USA Patriot Act and Section 702 of the FISA Amendments Act. *See* Weinstein et al., *supra* note 7, at 729–30.

[51] *See* Weinstein et al., *supra* note 7, at 745–46; Green, *Is Apple Picking a Fight?*, *supra* note 41. Those fears have begun to manifest, and tensions have escalated as law enforcement officials continuously encounter investigative obstacles due to heavily encrypted iPhones. *See* Barrett & Wakabayashi, *supra* note 17.

[52] *See* Weinstein et al, *supra* note 7, at 745; Barrett & Wakabayashi, *supra* note 17; Comey, *supra* note 11.

[53] *See In re Apple, Inc.*, 149 F. Supp. 3d at 347–48; Corn, *supra* note 10, at 1436–37; Barrett & Wakabayashi, *supra* note 17.

[54] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause . . . ."); *see* United States v. Jones, 132 S. Ct. 945, 949–50 (2012); Katz v. United States, 389 U.S. 347, 350–52 (1967) (holding that the Fourth Amendment "protects people, not places" from certain kinds of governmental intrusion, thus departing

only applies, however, where the target of government action has manifested an objectively reasonable expectation of privacy in the item or information subject to the search.[55] Once the protection is implicated, a particularized warrant based on probable cause is generally required before law enforcement officials may execute a search, unless one of several exceptions applies.[56] Where a validly substantiated warrant is obtained from a neutral and detached magistrate, there is a strong presumption that the subsequent search will be reasonable under the Constitution.[57]

In 2014, in *Riley v. California*, the U.S. Supreme Court held that the Fourth Amendment generally requires a warrant to search the digital data contained on a cellphone.[58] Even before *Riley*, however, many law en-

from the previous doctrine that the Fourth Amendment had its principle moorings in trespass laws).

[55] *See* California v. Greenwood, 486 U.S. 35, 39–40 (1988); *Katz*, 389 U.S. at 351–53; Wilson, *supra* note 1, at 9–10 (noting that this inquiry requires both a subjective manifestation of that expectation and an objective analysis as to whether that expectation is one that society would recognize as reasonable). For example, it has long been held that there is no reasonable expectation of privacy in information disclosed to third parties, whether they be individual or institutional. *See* United States v. Miller, 425 U.S. 435, 443 (1976); Hoffa v. United States, 385 U.S. 293, 303 (1966).

[56] *See* Kentucky v. King, 563 U.S. 452, 459 (2011); Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971); *see also* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("[B]ecause the ultimate touchstone of the Fourth Amendment is 'reasonableness,' the warrant requirement is subject to certain exceptions."); Groh v. Ramirez, 540 U.S. 551, 557 (2004) (holding that a valid warrant must provide particularity in both the place being searched and the object sought); John M.A. DiPippa, *Is the Fourth Amendment Obsolete? Restating the Fourth Amendment in Functional Terms*, 22 GONZ. L. REV. 483, 486 n.20 (1986/1987) ("There are at least seven [recognized] exceptions to the warrant requirement."); William Clark, Note, *Protecting the Privacies of Digital Life:* Riley v. California*, the Fourth Amendment's Particularity Requirement, and Search Protocols for Cellphone Search Warrants*, 56 B.C. L. REV. 1981, 1986–87 (2015) (discussing the particularity element of the warrant requirement, which is satisfied by articulable descriptions of "the place to be searched" and "the people or things to be seized" (quoting the Fourth Amendment)).

[57] *See* United States v. Leon, 468 U.S. 897, 913–14 (1984) (holding that "great deference" should be given to a magistrate's issuance of a warrant, but that deference does not preclude further inquiry into the circumstances surrounding its application and issuance); *see also* Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.' . . . In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." (quoting *Brigham City*, 547 U.S. at 403)); United States v. Ventresca, 380 U.S. 102, 106 (1965) ("[I]n a doubtful or marginal case a search under a warrant may be sustainable where without one it would fail."); United States v. Lemke, No. 08–216(1), 2008 WL 4999246, at *14 (D. Minn. Nov. 19, 2008) ("[T]he reviewing Court must not engage in a de novo review but, rather, should accord great deference to the decision of the Judicial Officer who issued the Warrant.").

[58] *Riley*, 134 S. Ct. at 2493 Although the actual question presented in *Riley v. California* was whether the search-incident-to-arrest exception to the warrant requirement justified the warrantless search of a cellphone, the unanimous opinion of the court has been widely interpreted as establishing a bright-line rule that a warrant is required before a cellphone may be searched. *See id.* at 2495; Clark, *supra* note 56, at 1996. The Court also noted that the exigent-circumstances exception would most likely still apply to cellphones, which may justify warrantless searches under certain circumstances. *See Riley*, 134 S. Ct. at 2494.

forcement officials regularly sought and obtained search warrants before searching seized cellphones.[59] Many have opined that recent and continuing advancements in device-encryption could pose a danger to public safety and threaten the time-honored functionality of the warrant requirement, if potentially probative evidence can no longer be lawfully obtained without the phone's password.[60] Some argue that an impenetrable barrier to lawful warrant executions is fundamentally inconsistent with the fulcrum of the Fourth Amendment.[61] These concerns fit neatly under the already existent problem of Going Dark, which signifies law enforcement's inability to access certain data and communications—in this case, for example, contents of encrypted electronic devices.[62] Some have deflected such criticism by suggesting there are methods available to authorities that would allow them to get into seized devices, such as obtaining the passcode from the phone's owner or utilizing cryptanalytic techniques.[63] The former solution may be a nullity, however, as the only federal appeals court to have ruled on the matter held that compelling the owner of an electronic device to divulge his or her password is precluded by the Fifth Amendment's Self-Incrimination Clause.[64] Furthermore, the viability of existing forensic techniques, such as brute-force, is

[59] *See In re* Search of White Apple iPhone, Model A1332, No. C–12–224M, 2012 WL 2945996, at *1–2, (S.D. Tex. Apr. 11, 2012) (denying government's application for a warrant to search defendant's iPhone, which had been taken into custody as a result of his arrest); *Lemke*, 2008 WL 4999246, at *7 (discussing the circumstances surrounding the search of a cellphone seized incident to an arrest, which included securing the cellphone in the arresting officer's desk until a warrant was obtained).

[60] *See* Corn, *supra* note 10, at 1439, 1455–56; Comey, *supra* note 11; Orin Kerr, *Apple's Dangerous Game*, WASH. POST (Sept. 19, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game [https://perma.cc/8VTN-UJFH]; Cyrus R. Vance Jr., Opinion, *Apple and Google Threaten Public Safety with Default Smartphone Encryption*, WASH. POST (Sept. 26, 2014), https://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html [https://perma.cc/C2GC-NPCU].

[61] Corn, *supra* note 10, at 1439 ("[T]he people have never had an absolute and unqualified right to privacy but instead a right to be secure against *unreasonable* government intrusions . . . .").

[62] *See* FINKLEA, *supra* note 6, at 8–9; Comey, *supra* note 11; *see supra* note 11 and accompanying text (discussing the Going Dark challenges that face law enforcement with increasingly robust encryption of data at rest).

[63] *See* FINKLEA, *supra* note 6, at 8, 11.

[64] *See In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1346–49 (11th Cir. 2012) (holding that forced decryption of a computer hard drive was precluded by the Self-Incrimination Clause, because production of a computer's password is testimonial communication); Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How Riley Matters*, 109 NW. U. L. REV. 1131, 1133 (2015); *see also* U.S. CONST. amend. V ("No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."); Wilson, *supra* note 1, at 27 (discussing the precarious state of the law with regards to compelled decryption). *See generally* J. Riley Atwood, *The Encryption Problem: Why the Courts and Technology Are Creating a Mess for Law Enforcement*, 34 ST. LOUIS U. PUB. L. REV. 407, 416–24 (2015) (discussing the development and current state of how federal courts approach compelled decryption).

difficult to fully ascertain because such techniques tend to be very device specific due to variable features, such as the auto-erase function.[65]

D. Apples and Oranges: Relevant, but Inapposite Federal Statutes

Currently, there is no federal statute that explicitly covers the propriety of compelling third-party manufacturers to bypass the passcodes of locked mobile devices to provide access for the government.[66] Nevertheless, there are two federal laws that arguably come close.[67] The first is the Stored Communications Act ("SCA"), which was enacted under Title II of the Electronic Communications Privacy Act ("ECPA") in 1986.[68] Among other things, the SCA governs when government actors may compel network service providers to disclose stored electronic communications.[69] This most likely does not apply to governmental requests for assistance in bypassing the lock-screen of devices, however, because the password itself is not an "electronic communication" *held* by the third-party service provider.[70]

[65] *See* FINKLEA, *supra* note 6, at 8; The Govt's Memorandum of Law in Support of Its Application for an Order Compelling Apple Inc. to Assist Law Enforcement Agents in Execution of a Search Warrant at 40–44, *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-01902) [hereinafter *Govt's District Court Brief*]. At least one undisclosed technique developed by a third party and provided to the government in *The San Bernardino Case*, has proven to be effective in accessing an iPhone 5C running iOS9, but its applicability to other situations is currently unknown. *See* Barrett, *supra* note 15; Palazzolo & Barrett, *supra* note 13. For example, the government claims that it cannot be used to access newer models of iPhones, such as the 5S or the 6. *See* Barrett, *supra* note 15.

[66] *See In re Apple, Inc.*, 149 F. Supp. 3d at 355, 363; Wilson, *supra* note 1, at 31–32; Christian Levis, Note, *Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 191, 204 (2011).

[67] *See In re Apple, Inc.*, 149 F. Supp. 3d at 356–58; Wilson, *supra* note 1, at 30–32. Furthermore, there are other provisions in the Electronic Communications Privacy Act ("ECPA") and the Foreign Intelligence Surveillance Act ("FISA") that require private firms to furnish technical assistance with court ordered interceptions, installation of pen registers, and acquisition of communication. *See* 18 U.S.C. §§ 2518(4), 3124(a) (2012); 50 U.S.C. § 1881(a)(h)(1)(A) (2012); van Hoboken & Rubinstein, *supra* note 50, at 525. All three provisions contain similar language, in that they require firms to provide "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference." van Hoboken & Rubinstein, *supra* note 50, at 525.

[68] *See* 18 U.S.C. §§ 2701–2712 (2012); Wilson, *supra* note 1, at 30–32. See generally Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267 (2013), for a more comprehensive account of the SCA's structure, applicability, and modern interpretation.

[69] *E.g.*, Melinda L. McLellan et al., *Wherever You Go, There You Are (With Your Mobile Device): Privacy Risks and Legal Complexities Associated with International "Bring Your Own Device" Programs*, 21 RICH. J.L. & TECH. 1, 1, 24 (2014). The Stored Communications Act ("SCA") applies to both "electronic communication service" ("ECS") providers, which includes telephone companies, and "remote computing service providers," which includes companies like YouTube. *E.g.*, Wilson, *supra* note 1, at 30–31.

[70] *See* Wilson, *supra* note 1, at 31–32; Reid Day, Comment, *Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services*,

Second, there is the CALEA, enacted in 1994, which mandates that telecommunications carriers, broadband, and Voice over Internet Protocol providers design their equipment, facilities, and services to ensure that their networks are technologically amenable to government wiretap orders.[71] This generally requires carriers to maintain built-in surveillance capabilities in their networks to allow the government to monitor and access communications in real-time.[72] Specifically, a carrier must be able to isolate and intercept wire and electronic communications transmitted within its network, and it must possess the capability to either deliver those communications to law enforcement personnel or enable the government access on its own.[73] It further requires carriers to facilitate authorized access to call-identifying information that is reasonably available to the carrier.[74] Furthermore, it mandates carriers to consult with transmission equipment manufacturers and support services as necessary to ensure compliance, and requires those manufacturers and support services to cooperate.[75] Lastly, CALEA only requires built-in

64 U. KAN. L. REV. 491, 502 (2015); *see also* 18 U.S.C. § 2510(12) (2012) ("'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or potooptical system that affects interstate or foreign commerce . . . ."). If it were, the password would be obtainable with a Rule 41 warrant. *See* 18 U.S.C. § 2703(a); Wilson, *supra* note 1, at 31–32. Interpretation of the SCA in the context of emerging technologies has been met with many challenges. *See* McLellan et al., *supra* note 69, at 24.

[71] 47 U.S.C. §§ 1001–10; *see In re* Order Requiring Apple, Inc. Assist in Execution of Search Warrant (*In re Apple—Preliminary Mem. and Order*), No. 1:15-mc-01902, 2015 WL 5920207, at *2–3 (E.D.N.Y. Oct. 9, 2015) (preliminary memorandum and order); van Hoboken & Rubinstein, *supra* note 50, at 526. The text of CALEA refers only to telecommunications carriers, which the Act defines as an "entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire," but also directs carriers to consult with equipment manufacturers and support services. 47 U.S.C. §§ 1001(8)(A), 1002(a), 1005(a); *see* Am. Council on Educ. v. FCC, 451 F.3d 226, 228 (D.C. Cir. 2006). CALEA also contains a provision, known colloquially as the "substantial replacement provision," which allows the FCC to expand the definition of "telecommunications carrier" to include emerging technologies that it finds substantially replace the functions of "the local telephone exchange service." *See* 47 U.S.C. § 1001(8)(B)(ii); *see also Am. Council on Educ.*, 451 F.3d at 229 (discussing the FCC's administrative expansion of CALEA to cover Voice-over-Internet Protocol technologies and broadband networks).

[72] *E.g.*, Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix—Doctrine to Follow*, 14 N.C. J. L. & TECH. 489, 536 (2013). CALEA tapers this mandate by limiting technological capability requirements to that which provides a "minimum of interference" with customer services and in a manner that respects the privacy of communications and information not authorized for interception. *See* 47 U.S.C. § 1002(a)(4)(A); van Hoboken & Rubinstein, *supra* note 50, at 526.

[73] *See* 47 U.S.C. § 1002(a); Van Hoboken & Rubinstein, *supra* note 50, at 526.

[74] *See* 47 U.S.C. § 1002(a)(2); *see also id.* § 1001(2) ("'[C]all-identifying information' means dialing or signaling information that identifies the origin, direction, destination, or termination of each of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.").

[75] *See* 47 U.S.C. § 1005.

capabilities for access, it is not a blanket authorization for governmental access, which must be predicated by some independent court order.[76]

One notable statutory limitation is that CALEA explicitly excludes from coverage "persons or entities insofar as they are engaged in providing information services," which includes internet service providers, email services, and electronic publishing services.[77] Secondly, carriers are not responsible for decrypting any encrypted communication unless the cryptosystem was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.[78] Therefore, CALEA does not apply to password encrypted devices and the underlying data at rest, because it is explicitly limited to the interception of real-time communications and call-identifying information transmitted by telecommunications carriers.[79]

The possibility of updating and expanding CALEA to cover companies like Apple and Google has been discussed by law enforcement and members of Congress since as early as 2009, but no proposed amendments to CALEA have ever been introduced by Congress.[80] Although CALEA only

[76] *See id.* §§ 1001(8)(C)(i); 1002(a); *Am. Council on Educ.*, 451 F.3d at 228 n.2. CALEA does not affect the scope of the government's powers to conduct wiretapping and surveillance, which is principally prescribed under Title III of the Omnibus Crime Control and Safe Streets Act ("the Wiretap Act") and the Foreign Intelligence Surveillance Act ("FISA"). *See Am. Council on Educ.*, 451 F.3d at 228 n.2; Christa M. Hibbard, Note, *Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance*, 64 FED. COMM. L.J. 371, 374–75 (2012). CALEA instead applies to technologies used by the carriers in their networks, and even requires companies to allow the FBI to review compliance modifications prior to their implementation. *See* Pell, *supra* note 72, at 536.

[77] 47 U.S.C. § 1002(b)(2)(A); *see Am. Council on Educ.*, 451 F.3d at 228; van Hoboken & Rubinstein, *supra* note 50, at 526; *see also* 47 U.S.C. § 1001(6)(A) ("'[I]nformation services' . . . means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications . . . [including] . . . electronic messaging services . . . ."). The FCC, which is charged with administering CALEA, has determined that "information services" under CALEA should be interpreted narrowly. *See* In the Matter of Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs., 20 FCC Rcd. 14989, 15000 (2005). Thus, when a single entity provides multiple types of services, CALEA applies to any telecommunications component of that entity's services, whereas it does not apply to any information-service component of those services. *See id.*

[78] *See* 47 U.S.C. § 1002(b)(3); van Hoboken & Rubinstein, *supra* note 50, at 526. A third statutory limitation, is that CALEA does not authorize a government agency to require electronic communication services, manufacturers of telecommunications equipment, or telecommunications support services to adopt "any specific design of equipment, facilities, services, features, or system configurations," or prohibit the adoption thereof. 47 U.S.C. § 1002(b)(1).

[79] *See* 47 U.S.C. § 1002; *In re Apple, Inc.*, 149 F. Supp. 3d at 355–57; Peter T. King, *Remembering the Lessons of 9/11: Preserving Tools and Authorities in the Fight Against Terrorism*, 41 J. LEGIS. 173, 178 (2014).

[80] *See* King, *supra* note 79, at 178–79. A proposal to expand CALEA to cover all communications service providers—including e-mail service providers, social networking sites, and peer-to-peer messaging services was drafted by the FBI and approved by the DOJ in or around 2009. *Id.* at 179. The proposal was never sent to Congress. *Id.* Discussions as late as 2012 had primarily been focused on encryption's debilitating effect on the government's ability to conduct wiretaps for e-mail ser-

pertains to wiretapping, the story behind its adoption and effect is analogous to the current challenges presented by enhanced encryption of data at rest.[81] Many federal officials seem to be in agreement that a legislative solution of some kind will eventually be needed.[82] Cryptographers and security experts have consistently cautioned against any legislatively mandated "back door" because it would materially weaken security.[83] The Obama administration indicated in October 2015 that it would not pursue legislation just yet, but would instead continue conversations with the tech industry, which have since remained ongoing amidst several congressional hearings.[84] In the interim, there are still phones that the government has seized that it cannot access, and federal prosecutors have largely turned to the judiciary for more immediate relief.[85] As early as 2008, prosecutors have sought and obtained

vices, social-networking sites, and peer-to-peer communication providers. *See* Devlin McCullagh, *FBI: We Need Wiretap-Ready Websites—Now*, CNET (May 4, 2012, 9:24 AM), http://www.cnet.com/news/fbi-we-need-wiretap-ready-web-sites-now [https://perma.cc/L3CU-QRX4]; *see also Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 14–15, 42–43 (2011) [hereinafter *Going Dark Part I*] (statement and testimony of Valerie Caproni, General Counsel, FBI) (discussing the problem facing law enforcement as being an inability to intercept certain communications in response to a court order, rather than directly suggesting CALEA should be expanded). There have been thoughts that an expansion of CALEA could address this issue; and proposals to expand its scope to cover all communication services, including internet and email, have been discussed. *See Going Dark Part I*, *supra*, at 42; van Hoboken & Rubinstein, *supra* note 50, at 502 & n.92.

[81] *See* Comey, *supra* note 11; *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 3–8. (2015) [hereinafter *Going Dark Part II*—Yates & Comey Statement] (statement of Sally Quillian Yates, Deputy Attorney General, DOJ & James Comey, Director, FBI).

[82] *See* Barrett & Wakabayashi, *supra* note 17 (discussing the hearing before the House Judiciary Committee in 2016, where both state and federal officials testified about potential solutions). *See generally* van Hoboken & Rubinstein, *supra* note 50, at 514–33 (discussing front door and back door access points, and the relationship between CALEA and cloud-computing).

[83] *See, e.g.*, Andy Greenberg, *Why Proposed State Bans on Phone Encryption Are Moronic*, SLATE (Jan. 29, 2016, 12:14 PM), http://www.slate.com/blogs/future_tense/2016/01/29/new_york_and_california_have_proposed_state_bans_on_phone_encryption.html [https://perma.cc/9VTE-S8GK].

[84] *See The Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. (2016) [hereinafter *Encryption Tightrope Hearing*] (statement of Rep. Goodlatte, Chairman, H. Comm. on the Judiciary); *World Wide Threats: Hearing Before the H. Permanent Select Comm. On Intelligence*, 114th Cong. (2016) (testimony of James Comey, Director, FBI); Barrett & Wakabayashi, *supra* note 17; Zakrzewski, *supra* note 5. On the state level, both California and New York have introduced bills that would ban the retail sale of smartphones incapable of being decrypted and unlocked by its manufacturer or operating system provider. *See* A.B. 1681, 2016 Cal. Assemb., Reg. Sess. (Cal. 2016); A.B. 8093, 2015 N.Y. Assemb., 238th Sess. (N.Y. 2015). Both bills have been viewed as an effort to entice the federal government to take steps to address the issue. *See* Greenberg, *supra* note 83.

[85] *See* Barrett & Wakabayashi, *supra* note 17 (noting that federal prosecutors are pursuing orders against Apple in various proceedings involving at least fifteen seized iPhones in unrelated criminal matters).

orders to direct Apple, and other unknown vendors, to provide technical assistance in gaining access to encrypted devices in over seventy cases.[86]

II. THE ALL WRITS ACT

In those seventy-plus cases, the government has filed its order-applications under a statute known as the All Writs Act, which has occasionally been used to order third-party assistance to the government in other similar contexts since the 1970s.[87] This Part discusses the legal authority behind the government's efforts to conscript third-party decryption assistance in order to execute device search warrants.[88] Section A of this Part provides a brief historical overview of the All Writs Act and background discussion of the Act as a source of injunctive relief.[89] Section B discusses specific requirements that must be satisfied by a party seeking an All Writs injunction in the federal district courts.[90] Section C discusses the federal courts' authority under the Act to compel third-party assistance to the government.[91]

A. Historical & Procedural Overview of the All Writs Act

The All Writs Act, codified in 28 U.S.C. § 1651(a), provides in its entirety: "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usage and principles of law."[92] The Act traces its lineage, in substance, back to two sections of the Judiciary Act of 1789.[93]

[86] *See In re Apple, Inc.*, 149 F. Supp. 3d at 348; Palazzolo & Barrett, *supra* note 13.

[87] *See In re* Order Requiring Apple, Inc. Assist in Execution of Search Warrant (*In re Apple, Inc.*), 149 F. Supp. 3d 341, 348 (E.D.N.Y. 2016); Palazzolo & Barrett, *supra* note 13; *see also* United States v. N.Y. Tel. Co., 434 U.S. 159, 172 174–78 (1977) (holding that a district court has authority under the Act to order public telephone companies to provide technical assistance to the FBI in order to execute a surveillance order).

[88] *See infra* notes 92–142 and accompanying text.

[89] *See infra* notes 92–108 and accompanying text.

[90] *See infra* notes 109–131 and accompanying text.

[91] *See infra* notes 132–142 and accompanying text.

[92] 28 U.S.C. § 1651(a) (2012). A "writ" is a court's written order commanding the addressee to do or refrain from doing some specified act in the name of a state or other competent legal authority. *Writ*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[93] *See* Judiciary Act of 1789, ch. 20, §§ 13–14, 1 Stat. 73, 81–82 (1789); *N.Y. Tel. Co.*, 434 U.S. at 172; Lonny Sheinkopf Hoffman, *Removal Jurisdiction and the All Writs Act*, 148 U. PA. L. REV. 401, 433 (1999). Sections 13 and 14 of the First Judiciary Act provided the ancestral influence for § 1651(a). *See* Sheinkopf Hoffman, *supra* note 93, at 401 n.4. In 1948, the two provisions were essentially consolidated into what is now referred to as the All Writs Act, promulgated in its current form in 28 U.S.C. § 1651(a), which substantially mirrors the language of section 14. 28 U.S.C. § 1651(a); *see* Michael D. Sousa, *A Casus Omissus in Preventing Bankruptcy Fraud: Ordering a Search of a Debtor's Home*, 73 OHIO ST. L.J. 93, 111–12, 111 n.114 (2012); *see also* Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 40–42 (1985) (discussing the legislative history of 28 U.S.C. § 1651 as being a consolidation of section 14 and various provisions without

The fundamental purpose of the All Writs Act has been to supply the federal courts with the procedural tools necessary to perform their duty and protect their respective jurisdictions.[94]

As interpreted by the U.S. Supreme Court, the All Writs Act empowers a federal court to issue any writ that may be "necessary or appropriate" to help effectuate a previously issued order.[95] For example, if parties of an action were free to ignore a court judgment or order, the issuing court's ability to perform its duties would be undermined.[96] Thus, if a litigant's conduct can be properly characterized as violating a previously issued court order, the issuing court has jurisdiction to enjoin that conduct.[97] Furthermore, this power may also extend to persons or entities who, though not parties to the original action or engaged in any wrongdoing, are in a position to frustrate the implementation of a court order or to thwart the administration of justice.[98]

substantial change in meaning or purpose). As a result of the 1948 revisions, the All Writs Act is the sole statutory authority on which a court may base its issuance of an extraordinary writ, with the exception of 28 U.S.C. § 2241(a) concerning writs of habeas corpus. *See* Sheinkopf Hoffman, *supra*, at 434–35.

[94] Harris v. Nelson, 394 U.S. 286, 300 (1969) ("This statute has served since its inclusion, in substance, in the original Judiciary Act as a 'legislatively approved source of procedural instruments designed to achieve 'the rational ends of law.'" (quoting Price v. Johnston, 334 U.S. 266, 282 (1948))); *see* Sousa, *supra* note 93, at 112–13; *see also* Wythe Holt *"To Establish Justice": Politics, the Judiciary Act of 1789, and the Invention of the Federal Courts*, 1989 DUKE L.J. 1421, 1507 (describing section 14, known as the "all-writs" provision, as "the most expansive and open-ended" provision in the First Judiciary Act, and discussing its versatility in application). Thus, some courts have characterized the All Writs Act as a partial codification of long-recognized equitable principles, which have allowed federal courts to effectuate their own previous decrees or judgments by injunctions or writs of assistance. *See* Wesch v. Folsom, 6 F.3d 1465, 1470 (11th Cir. 1993); Hamilton v. Nakai, 453 F.2d 152, 157 (9th Cir. 1971). Those instruments include the common-law writs of certiorari, injunction, prohibition, mandamus, and all other writs available at common law. *See* 3-27 MOORE'S MANUAL: FEDERAL PRACTICE AND PROCEDURE § 27.07 (Matthew Bender) [hereinafter 3-27 MOORE'S MANUAL].

[95] *N.Y. Tele. Co.*, 434 U.S. at 172; *see also id.* at 172–73 ("[U]nless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties, when the use of such historic aids is calculated in its sound judgment to achieve the ends of justice entrusted to it." (quoting Adams v. U.S. *ex rel.* McCann, 317 U.S. 269, 273 (1942))). In terms of form, only injunctive orders under the Act will be discussed in this Note, because the use of other common-law writs in federal district courts has been curtailed by the Federal Rules. *See* 3-27 MOORE'S MANUAL, *supra* note 94, § 27.07; *see also* FED. R. APP. P. 21 (providing procedural guidelines regarding writs of mandamus and prohibition); FED R. CIV. P. 81(b) (abolishing the writ of mandamus and scire facias at the federal district court level).

[96] *E.g. N.Y. Tel. Co.*, 434 U.S. at 188 (Stevens, J., dissenting in part).

[97] *See id.*; *Harris*, 394 U.S. at 299 (citation omitted) ("[The All Writs Act] has served . . . as a 'legislatively approved source of procedural instruments to achieve 'the rational ends of law.'" (quoting *Price*, 334 U.S. at 282)); Marshall v. Local Union No. 639, 593 F.2d 1297, 1302 (D.C. Cir. 1979).

[98] *N.Y. Tel. Co.*, 434 U.S. at 174. This prescribed reach to nonparties "encompasses even those who have not taken any affirmative action to hinder justice." *Id.*; *see also* United States v. Doe, 537 F. Supp. 838, 839 (E.D.N.Y. 1982) (using power under the All Writs Act to order a telephone company to supply telephone toll records); *In re* Order Requiring XXX, Inc. to Assist in

In the district courts, orders under the All Writs Act typically take the form of an injunction, and may only be issued when necessary to protect the court's underlying subject matter jurisdiction.[99] Thus, as courts with limited original jurisdiction, federal district courts can only issue orders under the Act in aid of that jurisdiction acquired on some independent ground.[100] Procedurally, the Act enables district courts to issue injunctions under two distinct circumstances: (1) to safeguard ongoing proceedings; and (2) to effectuate already-issued orders and judgments.[101] In either situation a district court's jurisdiction has already been established; thus, when some conduct threatens to undermine the court's abilities to perform its duties it may issue an "ancillary injunction" under the Act to enjoin that conduct and preserve its jurisdiction.[102]

The All Writs injunction is slightly distinct from alternative forms of injunctive relief, such as traditional injunctions and statutory injunctions.[103]

Execution of Search Warrant by Unlocking Cellphone (*In re XXX, Inc.*), No. 14 Mag. 2258, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014) (issuing an order under the All Writs Act directing a cellphone manufacturer to assist in the execution of a search warrant by "bypassing the lock screen" of subject's cellphone).

[99] *See* Klay v. United Healthgroup, Inc., 376 F.3d 1092, 1099–1100 (11th Cir. 2004); 1-10A MOORE'S MANUAL: FEDERAL PRACTICE AND PROCEDURE § 10A.05 [hereinafter 1-10A MOORE'S MANUAL] (discussing ancillary injunctions under the All Writs Act, which are used to prevent conduct that could frustrate the court's jurisdiction).

[100] *See* Clinton v. Goldsmith, 526 U.S. 529, 534–35 (1999); ITT Cmty. Dev. Corp. v. Barton, 569 F.2d 1351, 1358–59 (5th Cir. 1978); Dimitri D. Portnoi, Note, *Resorting to Extraordinary Writs: How the All Writs Act Rises to Fill the Gaps in the Rights of Enemy Combatants*, 83 N.Y.U. L. REV. 293, 301 (2008). Federal district courts have original federal question jurisdiction, diversity jurisdiction, and special statutory and supplemental jurisdiction under certain circumstances. 28 U.S.C. §§ 1331–1332, 1367(a) (2012); *see, e.g.*, 28 U.S.C. §§ 1337–1338, 1340 (2012) (providing district courts with original jurisdiction).

[101] *See Klay*, 376 F.3d at 1099; *Barton*, 569 F.2d at 1359–60 (noting that the All Writs Act permits a district court to issue any order "necessary to enable the court to try the issue [in a pending case] to final judgment" and "develop the material issues and to bring them to a complete resolution"); Fruquan Mouzon, *Forgive Us Our Trespasses: The Need for Federal Expungement Legislation*, 39 U. MEM. L. REV. 1, 17 (2008); *see also N.Y. Tel. Co.*, 434 U.S. at 172 (noting the long-recognized authority of the federal courts to issue orders under the All Writs Act to "effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained").

[102] *See Klay*, 376 F.3d at 1099, 1102; Phillips Beverage Co. v. Belvedere S.A., 204 F.3d 805, 806 (8th Cir. 2000); *see also* 1-10A MOORE'S MANUAL, *supra* note 99, § 10A.05 (defining "ancillary injunction" as an injunction "used by a federal court to sustain its jurisdiction"). The converse is also true, if lack of conduct would tend to undermine a court's ability to perform its duties, such as ignoring an order or judgment, the court may issue an injunction requiring the party to comply or carry out the terms of the judgment. *See N.Y. Tel. Co.*, 434 U.S. at 187 (Stevens, J., dissenting in part); *see also In re* Y & A Grp. Sec. Litig., 38 F.3d 380, 382 (8th Cir. 1994) ("All Writs Act indirectly confers on injunction beneficiaries the right to judicial enforcement.").

[103] *See Klay*, 376 F.3d at 1100–02; Portnoi, *supra* note 100, at 299–301. There are at least three different types of injunctions a federal court can issue: a "traditional injunction," a statutory injunction, or an injunction under the All Writs Act. *Klay*, 376 F.3d at 1097–99; *see* Portnoi, *supra* note 100, at 300. A traditional injunction can be issued as either interim or permanent relief predi-

First, a traditional injunction is predicated upon some cause of action, whereas an All Writs injunction is predicated upon some identifiable threat to the integrity of an ongoing proceeding, or previously issued order or judgment.[104] Secondly, the primary purpose of an All Writs injunction is to protect the integrity of the court and its jurisdiction, rather than to protect the rights of individuals.[105] That is not to say, however, that a district court may evade the more stringent requirements of other applicable forms of injunctive relief by purporting to issue an All Writs injunction.[106] The Act is firmly regarded as a remedy of last resort.[107] No one clear test or standard for the All Writs Act has been consistently articulated, but the general purpose and fundamental limitations underlying the Act have received relatively consistent, piecemeal application.[108]

cated upon a cause of action, whether it be an alleged breach of common law, statutory, or constitutional rights. *See Klay*, 376 F.3d at 1097; Portnoi, *supra* note 100, at 300. The second type of injunction is a "statutory injunction," which is where a statute either prohibits certain conduct or establishes certain rights enforceable through court injunction, and sets forth the standard for doing so. *See Klay*, 376 F.3d at 1098. The third type is an "All Writs Act injunction," and may be issued by a court whenever it is "calculated in [the court's] sound judgment to achieve the ends of justice entrusted to it." *Id.* at 1099–1100 (alteration in original) (quoting *Adams*, 317 U.S. at 273); *see, e.g.*, United States v. Yielding, 657 F.3d 722, 727 (8th Cir. 2011); *Barton*, 569 F.2d at 1358–59. Regardless of the form, an injunction may be either *mandatory*, which command performance, or *prohibitory*, which forbid or constrain certain acts. *See* Sanchez v. Esso Standard Oil Co., 572 F.3d 1, 20 (1st Cir. 2009); Louis Vuitton Malletier v. Dooney & Bourke, Inc., 454 F.3d 108, 114 (2d Cir. 2006); 1-10A MOORE'S MANUAL, *supra* note 99, § 10A.05.

[104] *See Klay*, 376 F.3d at 1100; Portnoi, *supra* note 100, at 300–01; *see also Barton*, 569 F.2d at 1359 ("Conversely, conduct not shown to be detrimental to the court's jurisdiction or exercise thereof could not have been enjoined under the [All Writs Act]." (alteration in original)). Although the two forms' functions are substantially the same, a court issuing an injunction under the Act need not consider the traditional four injunction requirements, because the injunction is ancillary to the original proceeding. *See Klay*, 376 F.3d at 1100–02

[105] *See Klay*, 376 F.3d at 1100; Portnoi, *supra* note 100, at 300–01. Thus, the scope of a court's authority to enjoin under the act largely depends on "the nature of the case before [it] and the legitimacy of the ends sought to be achieved through the exercise of the power." *Barton*, 569 F.2d at 1358–59 (alteration in original).

[106] *See* Schiavo *ex rel.* Schindler v. Schiavo, 403 F.3d 1223, 1229 (11th Cir. 2005); *Pa. Bureau of Corr.*, 474 U.S. at 43. If relief sought is in essence a preliminary injunction or a temporary restraining order, for example, the All Writs Act is not available because Rule 65 of the Rules of Civil Procedure provides for temporary restraining orders and preliminary injunctions. *See* FED. R. CIV. P. 65(a)-(b); *Schiavo*, 403 F.3d at 1229.

[107] *See* Brown v. Gilmore, 533 U.S. 1301, 1303 (2001); *In re* Application of U.S. for Order Authorizing Disclosure of Location Info. (*In re Application for Location Info. (D. Md.)*), 849 F. Supp. 2d 526, 583 (D. Md. 2011); Portnoi, *supra* note 100, at 299; *see also* Ohio Citizens for Responsible Energy, Inc. v. Nuclear Regulatory Comm'n, 479 U.S. 1312, 1313–14 (1986) ("[A]pplicant must demonstrate . . . relief is 'necessary or appropriate in aid of [the Court's] jurisdiction[n]." (alteration in original) (quoting 28 U.S.C. § 1651(a))).

[108] *See In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 580; Sousa, *supra* note 93, at 113; Portnoi, *supra* note 100, at 299.

B. The All Writs Act in the Federal District Courts: General Requirements

Generally, the All Writs Act imbues federal courts with flexible, inherently equitable powers subject to judicial discretion.[109] This discretion is informed by several fundamental limitations and equitable considerations.[110] Most courts and commentators have recognized four elements to consider, with some slight variation, before an All Writs order may be properly issued.[111] In short, an All Writs order may only be issued where (1) no other law applies; (2) the issuing court has jurisdiction over the underlying matter on an independent basis and the order is "in aid of" that jurisdiction; (3) exceptional circumstances are present that make issuance under the Act necessary or appropriate; and (4) the issuance of relief is done in conformity with the "usages and principles of law."[112]

The first limitation is derived from the Act's residual nature, as its authority may only be invoked as a gap-filling measure to order action not otherwise covered by statute.[113] Although no such limiting language explicitly appears in the statutory text, historically this notion is consistent with

[109] *See Clinton*, 526 U.S. at 537 ("The All Writs Act invests a court with a power essentially equitable . . . ."); *N.Y. Tel. Co.*, 434 U.S. at 173 (noting that the Court has consistently applied the Act flexibly); United States v. George, 676 F.3d 249, 253 (1st Cir. 2012) (noting that the flexible, inherently equitable powers imbued to the courts through the Act "are anchored in informed judicial discretion").

[110] *See* Sousa, *supra* note 93, at 113–14; Portnoi, *supra* note 100, at 297–98; *see also* Morrow v. District of Columbia, 417 F.2d 728, 736 (D.D.C. 1969) ("The Supreme Court has stressed the theme that the issuance of the writ is a matter of sound discretion.").

[111] *In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 580; Sousa, *supra* note 93, at 113–14; Portnoi, *supra* note 100, at 299–303.

[112] *See In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 582; Sousa, *supra* note 93, at 113–14; Portnoi, *supra* note 100, at 299–303. Although this area of the law is undertheorized in secondary literature, and no fully consistent articulation of the prerequisites for an All Writs Act injunction has been announced by the lower courts, this formulation can be reasonably construed from the statutory text of the Act and the Supreme Court's interpretation. *See* Portnoi, *supra* note 100, at 299. Additionally, potential constitutional implications must be considered in the context of a criminal proceeding or government investigation, but such a consideration is consistent with the fourth factor previously listed. *See In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 580–81; *see also* Portnoi, *supra* note 100, at 303 (noting that the only guidance the statute provides is that orders may only be issued that are "agreeable to the usages and principles of law"). To issue an injunction that would impede on the Fourth Amendment privacy rights of the target of a government investigation, for example, would not be agreeable to the usages and principles of law. *See In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 580–81.

[113] *See Pa. Bureau of Corr.*, 474 U.S. at 43 ("Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling."); *In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 580; Portnoi, *supra* note 100, at 298–99; *see also* Syngenta Crop Prot., Inc. v. Henson, 537 U.S. 28, 32 (2002) ("[T]he All Writs Act 'fill[s] the interstices of federal judicial power when those gaps threate[n] to thwart the otherwise proper exercise of federal courts' jurisdiction.'" (alteration in original) (quoting *Pa. Bureau of Corr.*, 474 U.S. at 41)).

congressional intent and the spirit of separation of powers.[114] In 1985, the U.S. Supreme Court made clear in *Pennsylvania Bureau of Correction v. United States Marshals Service*, that "[w]here a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling."[115] Thus, if a suitable remedy is available by some other means, the courts' authority under the Act should be precluded.[116]

Second, an order under the Act may only be issued "in aid of" the issuing court's jurisdiction.[117] Once jurisdiction is vested in a federal court on an independent basis, that court may invoke the All Writs act "to enter orders it deems necessary or appropriate to preserve and protect its jurisdiction."[118]

[114] *See Pa. Bureau of Corr.*, 474 U.S. at 41–42; Portnoi, *supra* note 100, at 298; *see also* Stevenson v. Tyco Int'l (US) Inc., No. 04-4037, 2006 WL 2827635, at *9 (S.D.N.Y. Sept. 29, 2006) (holding the All Writs Act inapplicable where the Federal Arbitration Act divests federal courts of jurisdiction where parties properly request arbitration); William F. Ryan, *Rush to Judgment: A Constitutional Analysis of Time Limits on Judicial Decisions*, 77 B.U. L. REV. 761, 777 n.66 (1997) ("Congress, too, has always recognized that the federal courts would inevitably encounter procedural gaps, and has in various ways empowered the courts to fill those voids. This is clearly the purpose of the famous All Writs Act . . . ."). Section 14 of the First Judiciary Act contained the limiting phrase "not specifically provided for by statute," but that language was removed in the 1948 recodification. *See Pa. Bureau of Corr.*, 474 U.S. at 41–42. The Supreme Court made clear in *Pennsylvania Bureau of Correction v. United States Marshals Service* that its omission from the All Writs Act was merely a "necessary change[] in phraseology," and the limitation was still applicable. *Id.* (quoting H.R. REP. No. 80-308, at A144 (1947)).

[115] *Pa. Bureau of Corr.*, 474 U.S. at 43; *see also Clinton*, 526 U.S. at 537 ("The All Writs Act invests a court with a power essentially equitable and, as such, not generally available to provide alternatives to other, adequate remedies at law."). The Court went on to add that any authority under the Act should be reserved for filling "statutory interstices," rather than issuing "ad hoc writs" whenever compliance with alternative procedures appears inconvenient or less appropriate. *Pa. Bureau of Corr.*, 474 U.S. at 41, 43.

[116] *See Clinton*, 526 U.S. at 537 (1999); *Pa. Bureau of Corr.*, 474 U.S. at 43; *see also Harris*, 394 U.S. at 298–301 (holding that the All Writs Act authorized an order to a party in a habeas corpus proceeding to answer interrogatories propounded by a state prisoner, after finding that no other statute addressed the relief being sought and an extension of the federal discovery rules would have been unsuitable); *In re* Application of the U.S. for an Order (1) Authorizing the Use of Pen Register and Trap and Trace Device, 396 F. Supp. 2d 294, 326 (E.D.N.Y. 2005) (declining to invoke the All Writs Act where existing statutes addressed the type of investigative orders sought by the government). This first factor has alternatively been characterized as requiring a showing of an "absence of alternative remedies." Portnoi, *supra* note 100, at 299; *see also* Sousa, *supra* note 93, at 113 (adopting Portnoi's articulation of the "absence of alternative remedies" requirement).

[117] *See Clinton*, 526 U.S. at 534–35; *In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581; Portnoi, *supra* note 100, at 301–02; *see also* Brittingham v. Comm'r, 451 F.2d 315, 317 (5th Cir. 1971) (noting that the All Writs Act does not create jurisdiction in the district courts, but empowers them to issue writs in aid of jurisdiction previously acquired on some independent ground).

[118] *E.g.*, *In re* Order Authorizing the Use of a Pen Register, 538 F.2d 956, 961 (2d Cir. 1976), *rev'd on other grounds, sub nom. N.Y. Tel. Co.*, 434 U.S. at 172; Portnoi, *supra* note 100, at 301–02; *see also* Procup v. Strickland, 792 F.2d 1069, 1073 (11th Cir. 1986) (en banc) ("Federal courts have both the inherent power and the constitutional obligation to protect their jurisdiction from conduct which impairs their ability to carry out Article III functions."). The Supreme Court has made clear that the All Writs Act is not a source of subject-matter jurisdiction in and of itself. *See*

This inquiry becomes slightly more involved where the relief sought is a further order to effectuate a previously issued order, warrant, or judgment.[119] In this context, there must be some previously issued court order, unable to be implemented, that necessitates a further order to aid in its execution.[120]

Third, after determining that no other law occupies the space and there is an independent basis for jurisdiction, courts consider whether issuance under the Act is "necessary or appropriate."[121] This has often required a showing of "exceptional circumstances" that makes relief necessary to protect the issuing court's jurisdiction.[122] This inquiry often involves a combination of some identifiable threat to a court's jurisdiction, such as refusal to comply with a previous order, and lack of readily available alternative mechanisms for mitigating that threat.[123] Further considerations in conduct-

United States v. Denado, 556 U.S. 904, 913–14 (2009); *Syngenta Crop*, 537 U.S. at 33. In the context of ongoing proceedings this is generally a subtle issue, as jurisdiction has clearly been established and orders under the Act may be directed to immediate parties if found necessary or appropriate to manage the case to a just resolution. *See N.Y. Tel. Co.*, 434 U.S. at 188 (Stevens, J., dissenting in part); *Barton*, 569 F.2d at 1359.

[119] *See N.Y. Tel Co.*, 434 U.S. at 172; *In re* U.S. for Order Directing Provider of Commc'n Serv. to Provide Tech. Assistance to Agents of DEA (*In re Order Provide Tech. Assistance to DEA (D. P.R.)*), 128 F. Supp. 3d 478, 483 (D. P.R. 2015) (refusing to issue an order under the All Writs Act where the government failed to assert the existence of a previously issued court order or warrant that would be frustrated by a third party's lack of cooperation).

[120] *See Klay*, 376 F.3d at 1100; *In re Order Provide Tech. Assistance to DEA (D. P.R.)*, 128 F. Supp. 3d at 483; United States v. X (*U.S. v. X*), 601 F. Supp. 1039, 1042–43 (D. Md. 1984); *see also* Mitsubishi Intern. Corp. v. Cardinal Textile Sales, Inc. 14 F.3d 1507, 1517 n.17 (11th Cir. 1994) ("Conduct not shown to be detrimental to the court's jurisdiction or exercise thereof cannot be enjoined under the Act.").

[121] *See N.Y. Tel Co.*, 434 U.S. at 173, 175; *In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581; *U.S. v. X*, 601 F. Supp. at 1042–43; Portnoi, *supra* note 100, at 302–03.

[122] *See Pa. Bureau of Corr.*, 474 U.S. at 44–45 (Stevens, J., dissenting); *In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581. The extraordinary nature of relief pursuant to the Act calls for courts to inquire whether the petition before them presents exceptional circumstances that make the Act's invocation necessary and appropriate. *See* Alabama v. U.S. Army Corps of Eng'rs, 424 F.3d 1117, 1132 n.22 (11th Cir. 2005) ("The exceptional circumstances that have supported injunctions against related proceedings under the All Writs Act are not present here."); Liles v. Del Campo, 350 F.3d 742, 746–47 (8th Cir. 2003) (affirming the district court's authority under the All Writs Act to enjoin related federal proceedings in order to preserve the settlement fund of defendants involved in a conditional nationwide class action, to avoid inconsistent results, and to preserve judicial resources); *U.S. v. X*, 601 F. Supp. at 1043 (finding exceptional circumstances where a defendant had "disappeared," efforts to locate him had been unsuccessful, and records collected under a pen register would likely lead to his whereabouts).

[123] *See Klay*, 376 F.3d at 1100; Portnoi, *supra* note 100, at 299–300. The Supreme Court has consistently maintained that the primary purpose of the Act is to enable courts to protect their jurisdiction. *See Clinton*, 526 U.S. at 534; *Harris*, 394 U.S. at 299; Sousa, *supra* note 93, at 113. In 1977, in *United States v. New York Telephone Co.*, Justice White, writing for the majority of the Supreme Court, rejected the dissent's attempt to draw a distinction between orders in aid of a court's own duties and jurisdiction and orders designed to better enable a party to effectuate his or her own rights and duties. *See N.Y. Tel. Co.*, 434 U.S. at 175 n.23 ("[C]ourts normally exercise their jurisdiction only in order to protect the legal rights of parties."). Thus, although the Act is not

ing this inquiry include whether there are less intrusive means available to accomplish the purpose of the request; whether other means have been attempted and were unsuccessful; and the likelihood that issuance of an injunction under the Act will successfully accomplish the purported goal of the requested order.[124] Overall, the inquiry is a flexible one, but subject to sound discretion.[125] For example, in *Pennsylvania Bureau of Correction*, the Court held that the All Writs Act did not authorize a district court to order the U.S. Marshals Service to transport and supervise a witness being held in a state correctional custody to effectuate a previously issued habeas corpus order.[126] The Court concluded that the district court was not authorized to do so because no "exceptional circumstances" were demonstrated that suggested the state could not handle transporting the witness to the federal courthouse itself.[127]

Fourth, after finding sufficient exceptional circumstances that make an All Writs injunction necessary or appropriate, a court must fashion a reme-

broadly available as a remedy to protect a parties rights, the Act's purpose of preserving the issuing court's jurisdiction most often has the simultaneous effect of protecting parties' rights. *See id.*

[124] *See In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581–82.

[125] *See Klay*, 376 F.3d at 1100 ("A court may grant relief under the Act whenever it is 'calculated in [the court's] sound judgment to achieve the ends of justice entrusted to it,' and not only when it is 'necessary in the sense that the court could not otherwise physically discharge its . . . duties.'" (alteration in original) (quoting *Adams*, 317 U.S. at 273)); *see also* United States v. Catoggio, 698 F.3d 64, 67 (2d Cir. 2012) (citation omitted) ("[C]ourts have significant flexibility in exercising their authority under the Act.").

[126] *See Pa. Bureau of Corr.*, 474 U.S. at 43. The Court found that the pertinent habeas corpus provision at issue did not empower a court to direct third parties, who are neither custodians nor parties to the litigation, to bear the cost of producing the prisoner in a federal court. *See id.* at 39.

[127] *See id.* at 43. The Court left open the question of whether certain exceptional circumstances, such as serious security risks, may render traditional habeas statutes inadequate and justify a court's invocation of the All Writs Act to transport state prisoners. *See id.* Some lower courts have interpreted this language to suggest that issuance under the All Writs Act is only authorized when circumstances demonstrate an exceptional need for its invocation, although prior courts tended to apply the All Writs Act in the same manner. *See In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581–82; *In re* Application of U.S. for Order Directing X to Provide Access to Videotapes (*In re Order X to Provide Access to Videotapes (D. Md.))*, No. 03-89, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (finding sufficient exceptional circumstances present where arrest warrant had issued for defendant, agent stated that defendant had disappeared, efforts to locate defendant had been unsuccessful, and it was likely that an order under the Act directing nonparty to provide access security videotapes would provide information regarding defendant's whereabouts); *U.S. v. X*, 601 F. Supp. at 1042–43 (finding exceptional circumstances where a defendant had "disappeared," efforts to locate him had been unsuccessful, and an order directing third-party service provider to disclose records collected under a pen register would likely lead to his whereabouts because he was likely to use his phone to contact his family); *see also* Davis v. Glanton, 107 F.3d 1044, 1047 n.4 (3d Cir. 1997) (noting that a district court may only invoke the All Writs Act to remove an otherwise unremovable state court action when there is a showing of "exceptional circumstances").

dy that is "agreeable to the usages and principles of law."[128] This largely depends on the context in which the order is being issued, but generally, any order issued under the Act cannot offend established common law principles relative to the particular relief being sought, or otherwise be in violation of any statutory or constitutional provision.[129] For example, in the context of criminal proceedings or government investigations, courts must determine whether any constitutional provisions are implicated by the proposed order.[130] Where no Fourth Amendment privacy rights or other constitutional issues are implicated, however, courts have invoked the All Writs Act to order third-party assistance in effectuating previously issued search and arrest warrants.[131]

[128] 28 U.S.C. § 1651(a); *see* Sousa, *supra* note 93, at 114; Portnoi, *supra* note 100, at 303; *see also* Riggs v. Johnson, 73 U.S. (6 Wall.) 166, 190, 194 (1867) (noting that the single restriction on the courts' authority to exercise its jurisdiction is that the form and mode of process be agreeable to the principles and usages of law as known to both common law and the law of the various states at the time of the Act's enactment).

[129] *See* United States v. Perry, 360 F.3d 519, 534 (6th Cir. 2004); Sousa, *supra* note 93, at 114; Portnoi, *supra* note 100, at 303; *see also* Paramount Film Distrib. Corp. v. Civic Ctr. Theatre, Inc., 333 F.2d 358, 360 (10th Cir. 1964) ("The exercise of the power [under the All Writs Act] . . . is necessarily one of discretion, and is in accordance with the established principles relative to the particular writ which is sought." (alteration in original)). *But see In re Apple, Inc.*, 149 F. Supp. 3d at 357–59. (declining to adopt the interpretation of "agreeable to the usages and principles of law" as meaning anything not prohibited by law; and instead adopting a construction meaning "consonant with both the manner in which the laws were developed . . . and the manner in which the laws have been interpreted and implemented"). When issuing an injunction pursuant to the Act, courts are not authorized to issue injunctive relief "beyond what has traditionally been exercised by courts of equity." *See* Papadopoulos v. Sidi, 547 F. Supp. 2d 1262, 1270 (S.D. Fla. 2008) (quoting Rosen v. Cascade Intern., Inc., 21 F.3d 1520, 1528 n.15 (11th Cir. 1994)).

[130] *See Perry*, 360 F.3d at 534; *In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 580–81. The Fourth and Fifth Amendments are the constitutional provisions most likely to be implicated with the issuance of a court order to provide information or perform some action, such as assisting in the execution of a search warrant. *See In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581; *supra* notes 56–62 and accompanying text (discussing the applicability of the Fourth and Fifth Amendment with respect to government searches of cellphones). The Act does not relieve the government of its burden of establishing probable cause and complying with warrant requirements where constitutionally protected information is sought. *See In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581. Just as litigants may not sidestep statutory requirements by resorting to motion under the All Writs Act, the government may not sidestep constitutional restraints by seeking relief under the Act. *See Syngenta Crop*, 537 U.S. at 32–33; *In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581.

[131] *See In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581; *U.S. v. X*, 601 F. Supp. at 1042–43; *see also In re Order X to Provide Access to Videotapes (D. Md.)*, 2003 WL 22053105, at *2 (ordering production of video surveillance of public areas in an apartment complex, finding no reasonable expectation of privacy on the part of the tenants or their hallway visitors, and cooperation by the apartment complex would not be burdensome); *Doe*, 537 F. Supp. at 839–40 (issuing an order under the All Writs Act authorizing the production of toll records finding no reasonable expectation of privacy on the part of the subscribers).

C. Compelling Third Parties to Provide Assistance to the Government

The All Writs Act can be used to order nonparties to either assist or refrain from frustrating a previously issued warrant, even where there has been no affirmative interference.[132] In 1977, in *United States v. New York Telephone Co.*, the U.S. Supreme Court held that a district court had authority under the Act to issue an order requiring a public telephone company to provide technical assistance to the FBI in its effort to install a pen register on two telephone lines pursuant to a previously issued warrant.[133] The Court determined that the Act authorized the district court to issue the second order directing assistance, because it was necessary to prevent the warrant from being nullified, thus aiding in the courts jurisdiction to enable the authorized surveillance.[134] This determination hinged on the Court's conclusion that the telephone company was not a third party "so far removed" from the underlying investigation that its assistance could not be permissibly compelled.[135] The Court further noted that compliance would require

[132] *See N.Y. Tel. Co.*, 434 U.S. at 174; United States v. Mountain States Tel. & Tel. Co., 616 F.2d 1122, 1128 (9th Cir. 1980); Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979); *see also* Ass'n for Retarded Citizens of Conn., Inc. v. Thorne, 30 F.3d 367, 370 (2d Cir. 1994) ("By power of the All Writs Act, [a court] may require the compliance of nonparties in order to ensure that its legally-mandated directives are not frustrated." (alteration in original)); *Doe*, 537 F. Supp. at 839 (using the All Writs Act to order telephone company to supply telephone toll records in order to help effectuate a bench warrant for defendant's arrest); *In re XXX, Inc.*, 2014 WL 5510865, at *1–2 (issuing an order under the All Writs Act directing cellphone manufacturer to assist in the execution of a search warrant by "bypassing the lock screen" of subject's cellphone).

[133] *See N.Y. Tel. Co.*, 434 U.S. at 174–78. A "pen register" is a device used to record numbers dialed on a telephone by measuring electronic impulses caused when the dial of the telephone is released. *See id.* at 161 n.1. The case before the Court arose from the telephone company's refusal to fully comply with a previously issued order from the district court, which directed it to furnish the FBI all information, facilities, and technical assistance necessary to use the pen registers unobtrusively. *Id.* at 162. The FBI contended that it needed the assistance of the company in order to successfully install the pen register on the target lines without alerting the suspects. *See id.* at 162–63.

[134] *See id.* at 175 & n.23. The court noted that there was no conceivable way the FBI could install the pen register on its own without tipping off the targets of the investigation. *See id.* Before reaching this conclusion, the Court rejected the telephone company's argument that pen registers may only be authorized in conformity with Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("The Wiretap Act"). *See id.* at 165–67; Brian L. Owsley, *Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 195 (2014). The Court concluded that Title III was only concerned with orders authorizing "*interception* of wire communication," and that pen registers did not fit within the meaning of the statute because they only disclose the telephone numbers that have been dialed. *See N.Y. Tel. Co.*, 434 U.S. at 166–67.

[135] *See N.Y. Tel. Co.*, 434 U.S. at 174–75 ("[I]t can hardly be contended that the [c]ompany . . . had a substantial interest in not providing assistance."). In applying this standard, the U.S. Court of Appeals for the Second Circuit has determined that "the All Writs Act requires no more than that the persons enjoined . . . have the 'minimum contacts' that are constitutionally required under due process." United States v. Int'l Bhd. of Teamsters, 907 F.2d 277, 281 (2d Cir. 1990); *see* United States v. Mason Tenders Dist. Council of Greater N.Y., 205 F. Supp. 2d 183, 188 (2d

minimal effort on the company's part, and the compelled assistance would not disrupt the company's operations.[136] Furthermore, the Court also recognized the limits to the district court's authority to issue such orders, and noted that "unreasonable burdens may not be imposed."[137]

Although the practical import of *New York Telephone Co.* in the context of pen-register surveillance has largely dissipated, the Court's rationale regarding the All Writs Act has survived.[138] *New York Telephone Co.* still stands for the contention that the All Writs Act empowers federal courts to order a nonparty to an investigation to provide technical assistance to effectuate a prior order or warrant.[139] Despite this purported authority, lower

Cir. 2002). *But see In re Apple, Inc.*, 149 F. Supp. 3d at 368 (concluding that the requisite "minimum contacts," for the purposes of establishing personal jurisdiction, and the "too far removed" standard articulated in *New York Telephone Co.* are not coextensive).

[136] *N.Y. Tel. Co.*, 434 U.S. at 175. The Court rejected the concern that such a holding could establish an undesirable precedent for federal courts' authority to impress unwilling aid on third parties. *See id.* at 164, 175 n.24. The Court noted that the conviction that private citizens have a duty to provide assistance to law enforcement officials in necessary situations has been generally accepted by common-law traditions. *See id.* at 175 n.24.

[137] *Id.* at 172. In the wake of *New York Telephone Co.*, lower courts recognized that such assistance orders cannot be compelled without providing the target of the order a right to be heard. *See Mountain States Tel.*, 616 F.2d at 1132–33; *In re* Installation of a Pen Register or Touch-Tone Decoder & Terminating Trap (*In re Pen Register or Touch-Tone (3d Cir.)*), 610 F.2d 1148, 1157 (3d Cir. 1779). These three aforementioned factors—(1) how "far removed" the target of the order is from the underlying matter; (2) the amount of effort required for the requested action, and its potential disruption to business operations; and (3) the necessity of the order in aiding the court's jurisdiction—have been referred to as the *New York Telephone Co.* "discretionary factors." *See In re Apple, Inc.*, 149 F. Supp. 3d at 363–64. The degree of permissible burden is ultimately up to the district court's discretion, but at least one federal appeals court has directed lower courts to give considerable weight to the "*sui generis* character" of the technical assistance requested and the extent to which the target entity is regulated. *See Mountain States Tel.*, 616 F.2d at 1132.

[138] *See In re* Application of U.S. for Order Authorizing (1) Installation and Use of Pen Register and Trap Device or Process (*In re Application of U.S. (S.D. Tex)*), 441 F. Supp. 2d 816, 830–31 (S.D. Tex. 2006). Due to subsequent developments in federal case law and legislation, the All Writs Act soon became obsolete in the context of pen-register surveillance, which has been regulated by the Electronic Communications Privacy Act ("ECPA") since 1986. *See* 18 U.S.C. §§ 3121–3127 (2012); Smith v. Maryland, 442 U.S. 735, 741 (1979); *In re Application of U.S. (S.D. Tex)*, 441 F. Supp. 2d at 831; Owsley, *supra* note 134, at 196. Nothing in the ECPA or its history suggests dissatisfaction with either the holding or rationale of *New York Telephone Co. See In re Application of U.S. (S.D. Tex)*, 441 F. Supp. 2d at 818–19, 831.

[139] *See, e.g.*, *In re XXX, Inc.*, 2014 WL 5510865, at *1–2; *see also* United States v. Fricosu, 841 F. Supp. 2d 1232, 1238 (D. Col. 2012) (issuing an order under the All Writs Act requiring defendant to provide password to encrypted computer seized pursuant to a search warrant). Some lower courts have been skeptical to endorse such an expansive view of the judiciary's authority under the Act. *See In re* Order Requiring Apple, Inc. Assist in Execution of Search Warrant (*In re Apple—Preliminary Mem. and Order*), No. 1:15-mc-01902, 2015 WL 5920207, at *7 (E.D.N.Y. Oct. 9, 2015) (preliminary memorandum and order). Others have issued All Writs orders in support of previously issued warrants in a wide variety of contexts *See Mountain States Tel.*, 616 F.2d at 1129–30 (affirming the district court's order directing a phone company to assist with a trap and trace device); *In re Pen Register or Touch-Tone (3d Cir.)*, 610 F.2d at 1155 (same); *In re Order X to Provide Access to Videotapes (D. Md.)*, 2003 WL 22053105, at *3 (ordering a landlord to pro-

courts have generally held that procedural guarantees of due process require notice and a hearing on the issue of burdensomeness before assistance can be compelled. [140] An order shall not issue if the assistance sought would be unreasonably burdensome to the nonparty.[141] The degree of burdensomeness can be determined by balancing the government's need for assistance against the nonparty's interest in its own autonomy.[142]

III. SOUR APPLES: APPLE FINALLY BUCKS GOVERNMENT'S ORDER APPLICATIONS UNDER THE ALL WRITS ACT

On October 8, 2015, in the U.S. District Court for the Eastern District of New York, the government sought an order, pursuant to the All Writs Act, to direct Apple to bypass the lock-screen passcode of an iPhone 5s running on iOS 7, in order to effectuate a previously issued search warrant.[143] In a

vide access to security camera videotapes); United States v. Hall, 583 F. Supp. 717, 722 (E.D. Va. 1984) (ordering a credit card company to produce customer records); *U.S. v. X*, 601 F. Supp. at 1042–43 (same); *Doe*, 537 F. Supp. at 839–40 (ordering a phone company to produce telephone toll records).

[140] *See Mountain States Tel.*, 616 F.2d at 1132–33; *In re Pen Register or Touch-Tone (3d Cir.)*, 610 F.2d at 1157; *In re XXX, Inc.*, 2014 WL 5510865, at *2. To the extent the nonparty believes the order to be unduly burdensome, or that it should be reimbursed for expenses, courts have noted that the order should contain clear notice that the opportunity for objection is available. *See In re XXX, Inc.*, 2014 WL 5510865, at *2.

[141] *See N.Y. Tel. Co.*, 434 U.S. at 172; *In re Pen Register or Touch-Tone (3d Cir.)*, 610 F.2d at 1157; *see also In re* U.S. for Order Authorizing Roving Interception of Oral Commc'ns, 349 F.3d 1132, 1145 (9th Cir. 2003) ("The obligation of private citizens to assist law enforcement, even if they are compensated for the immediate costs of doing so, has not extended to circumstances in which there is a complete disruption of a service they offer to a customer as part of their business . . . ."); *In re Apple—Preliminary Mem. and Order*, 2015 WL 5920207, at *6 (discussing case law in which courts have considered the extent of intrusion that constitutes "unreasonably burdensome").

[142] *See N.Y. Tel. Co.*, 434 U.S. at 174–75; *In re Pen Register or Touch-Tone (3d Cir.)*, 610 F.2d at 1155. Relevant factors for determining reasonableness have included: (1) the likelihood of obtaining probative evidence; (2) available alternatives for accessing the information; (3) the extent to which assistance would disrupt operations or a commercial service; (4) the extent to which the invasiveness implicated by the execution of the order can be curtailed; (5) whether there is probable cause that the nonparty's facilities are being used for a criminal purpose; (6) whether the nonparty operates in a regulated industry; and (7) the likelihood that the nonparty can be compensated for assistance. *See N.Y. Tel. Co.*, 434 U.S. at 174–75; *In re Pen Register or Touch-Tone (3d Cir.)*, 610 F.2d at 1155 (finding All Writs Act assistance order to be appropriate and not overly burdensome where refusal would completely preclude execution of the warrant; assistance would cause "minimal disruption of normal operations;" and the telephone companies at issue would be fully compensated); *see also Mountain States Tel.*, 616 F.2d at 1133 (providing a variation of those factors in dicta).

[143] *In re* Order Requiring Apple, Inc. Assist in Execution of Search Warrant (*In re Apple—Preliminary Mem. and Order*, No. 1:15-mc-01902, 2015 WL 5920207, at *1 (E.D.N.Y. Oct. 9, 2015) (preliminary memorandum and order); *In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 33. The underlying warrant had been issued on July 6, 2015, by a U.S. Magistrate judge in the Eastern District of New York, and authorized the government to search the phone for

memorandum and order on October 9, 2015, the court questioned the government's assertion that the Act supported the relief being sought, noting that the relied-upon authority, particularly the 1977 U.S. Supreme Court case, *United States v. New York Telephone Co.*, suggested that it did not.[144] On February 29, 2016, following further briefing and argument on the propriety of the Act's authority and the issue of burdensomeness, the court issued a final ruling denying the government's application.[145] On March 7, 2016, the government appealed U.S. Magistrate Judge James Orenstein's decision to the District Court, however, it subsequently withdrew its application altogether after reporting that an unidentified individual had provided it with the passcode to the phone at issue.[146] Section A of this Part discusses Judge Orenstein's decision in *In re Order Requiring Apple, Inc. Assist in Execution of Search Warrant* ("*In re Apple, Inc.*").[147] Section B briefly discusses the larger significance of the holding, as almost a dozen All-Writs-order applications against Apple were pending before other federal magistrates across the country at the time the ruling was entered.[148]

evidence related to the possession and distribution of methamphetamine. *See In re* Order Requiring Apple, Inc. Assist in Execution of Search Warrant (*In re Apple, Inc.*), 149 F. Supp. 3d 341, 345–46 (E.D.N.Y. 2016). After failing to access the phone themselves due to the phone's security features, government agents sought assistance from Apple. *Id.* At that time, Apple indicated that it would comply with the request if the government first obtained a court order pursuant to the process outlined on the company's website, and made no objection to the propriety of the proposed order or the requested assistance. *See id.* at 346. Apple later submitted its initial opposition on October 22, 2015, after being invited to do so by the court. *See id.* at 346–47. At a hearing following issuance of Judge Orenstein's initial Memorandum and Order on October 9, 2015, the government clarified that what it was really seeking was "technical assistance," including "bypass and process information required from Apple's servers." *In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 68–69.

[144] *See In re Apple—Preliminary Mem. and Order*, 2015 WL 5920207, at *3, 5–7. Specifically, Judge Orenstein concluded that the opinion in *United States v. New York Telephone Co.* failed to support the government's motion, in light of the distinguishing characteristics between that case and the present matter. *See id.* at *5–6 (distinguishing *New York Telephone Co.* on the grounds that Apple did not have present control over the device at issue; that Apple is not a regulated public utility, and may have a discernable economic interest in not providing assistance; and that nothing on the record indicated that Apple regularly performed the requested service as part of its own operations or that it was even possible).

[145] *See In re Apple, Inc.*, 149 F. Supp. 3d at 346–47, 349.

[146] Letter Updating the Court and the Parties by the U.S., *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-01902). Accordingly, the court denied the government's application as moot. Order as to Appeal of Magistrate Judge Decision to District Court, *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-01902).

[147] *See infra* notes 149–160 and accompanying text.

[148] *See infra* notes 161–170 and accompanying text.

A. Magistrate Judge Orenstein: Placing the Apple Out of Reach

Judge Orenstein's principle holding was that the All Writs Act did not authorize the relief being sought, because an order compelling Apple to provide unwilling technical assistance would not be "agreeable to the usages and principles of law," as the Act demands.[149] Judge Orenstein based this conclusion on a finding that Congress had sufficiently considered legislation that would require governmental access to encrypted devices but has declined to adopt it.[150] Accordingly, Judge Orenstein concluded that granting relief under the Act would essentially be legislative in nature and repugnant to the doctrine of separation of powers.[151]

Before reaching its conclusion, Judge Orenstein engaged in the statutory construction of the "usages and principles" provision, finding that federal case law offered little guidance on the matter.[152] In so doing, Judge Oren-

[149] *See In re Apple, Inc.*, 149 F. Supp. 3d at 349, 363–64. Before reaching his conclusion, Judge Orenstein quickly conceded that issuance of an order under the circumstances would normally be "necessary or appropriate" in aid of the court's jurisdiction, because ordering such assistance is not specifically proscribed by Congress and an order would be needed to effectuate the validly issued warrant to search the device. *See id.* at 349–50. Judge Orenstein may have applied the doctrine in a slightly different manner than what was previously discussed in this Note, but it is not clear that his application was entirely correct. *See* Orin Kerr, *The Weak Main Argument in Judge Orenstein's Apple Opinion*, Opinion, WASH. POST (Mar. 2, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/03/02/the-weak-main-argument-in-judge-orensteins-apple-opinion [https://perma.cc/82CH-YVWH] (expressing dissatisfaction with the legal analysis employed by Judge Orenstein and arguing that Judge Orenstein improperly treated the statutory language as if it had not been previously constructed and interpreted it differently than it had been in the past by the U.S. Supreme Court).

[150] *See In re Apple, Inc.*, 149 F. Supp. 3d at 355–57, 360–61, 363. Judge Orenstein's justification of his decision was largely a result of its construction of the "usages and principles" provision. *See id.* 357–59; Kerr, *supra* note 149.

[151] *See In re Apple, Inc.*, 149 F. Supp. 3d at 349–50, 360–61, 370 n.36. Judge Orenstein noted that granting authority to the executive branch that Congress decided to withhold would be an unwarranted expansion of the Act's original purpose of ensuring the "smooth functioning" of the judiciary itself. *See id.* at 360–61; *see also* Holt, *supra* note 94, at 1507–08 (describing section 14, known as the "all-writs" provision, as "the most expansive and open-ended" provision in the First Judiciary Act). To be sure, writs have routinely been issued for "minor" administrative purposes from the beginning, but have also been reserved to be used to deal with "matters of great moment" through the Act's open-ended language. Holt, *supra* note 94, at 1507.

[152] *See In re Apple, Inc.*, 149 F. Supp. 3d at 352, 357–59. *But see* Bank of the United States v. Halstead, 23 U.S. (10 Wheat.) 51, 56 (1825) (finding the provision "embraces writs sanctioned by the principles and usages" under common law, but is not so limited); Kerr, *supra* note 149 (analyzing the Court's interpretation of the Act in *United States v. Halstead* and other cases, and concluding that the Court has consistently interpreted the Act to convey broad authority to the federal courts to issue writs beyond the forms available at common law, which will only be limited if Congress acts to do so). Judge Orenstein considered several cases in a footnote, but determined that in those cases the "usages and principles" provision was mainly concerned with whether the form of the writ sought was available under common law. *See In re Apple, Inc.*, 149 F. Supp. 3d at 353 n.10 (citing United States v. Hayman, 342 U.S. 205, 221 n.35 (1952) and Rawlins v. Kansas, 714 F.3d 1189, 1196 (10th Cir. 2013)).

stein determined that the most apt interpretation of the phrase was to permit only those orders that are "consonant with both the manner in which the laws were developed . . . and the manner in which the laws have been interpreted and implemented . . . ."[153] In recognizing the Act's overall residual nature, Judge Orenstein then turned to potentially relevant legislation to determine whether a statutory gap had emerged that would make relief under the Act appropriate.[154] He agreed with both parties that the Communication Assistance to Law Enforcement Act ("CALEA") does not require a company like Apple to provide assistance in this context, but diverged with the government's position by concluding that the omission reflects a conscious choice rather than simple oversight.[155] Judge Orenstein reasoned that CALEA is part of a larger, comprehensive scheme, and that scheme delineates the boundaries within which law enforcement may seek access to data in-motion and data at-rest.[156] He concluded that an absence of an affirmative obligation on a company like Apple to assist in accessing data at rest is sufficient to imply a legislative decision to prohibit the imposition of such a duty.[157]

[153] *In re Apple, Inc.*, 149 F. Supp. 3d at 358. Judge Orenstein explicitly rejected the meaning the government had ascribed the provision, which would allow an All Writs order to issue so long as it is "consistent with" the law, as in not prohibited by statute. *See id.* at 362, 370; The Govt's Post-Hearing Brief at 7, *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-01902) [hereinafter *Govt's Post-Hearing Brief*].

[154] *See In re Apple, Inc.*, 149 F. Supp. 3d at 354–58. Specifically, Judge Orenstein noted that the boundaries of the Act's gap-filling function could be easily drawn at two ends: (1) the Act cannot be interpreted to empower courts to do something already specifically authorized by another statute, and (2) it cannot be interpreted to authorize something specifically prohibited by another statute. *See id.* (citing Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985) ("Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling.").

[155] *See id.* 355–57, 363. To be sure, the Communication Assistance to Law Enforcement Act ("CALEA") only applies to the real-time interception of communications, whereas the underlying warrant authorized the search of data at rest, so it is likewise arguable that CALEA is not relevant to the underlying matter. *See* 47 U.S.C. § 1002 (2012); King, *supra* note 79, at 178. Judge Orenstein acknowledged this distinction, but found it irrelevant because Congress could have and did enact statutes regulating collection of data at rest elsewhere. *See In re Apple, Inc.*, 149 F. Supp. 3d at 356–57 (citing the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–2712 (2012)).

[156] *In re Apple, Inc.*, 149 F. Supp. 3d at 356–57. Judge Orenstein further noted that if that is what Congress intended, it could have incorporated such an obligation as it had elsewhere. *See id.* at 356–58; *see also* 18 U.S.C. §§ 2518(4); 3123(b)(2) (2012) (requiring private parties to assist in the execution of wiretaps and pen registers under certain circumstances); 18 U.S.C. § 2703(f)(1) (2012) (requiring providers of electronic communication services to, upon request, preserve all records and other evidence in its possession for government access pending proper court authorization).

[157] *See In re Apple, Inc.*, 149 F. Supp. 3d at 356–58, 363. In further support of his conclusion that Congress had sufficiently considered the issue, Judge Orenstein cited to several specific instances in which the Going Dark issue had been placed before Congress and legislative solutions had been discussed. *See id.*; *In re Apple—Preliminary Mem. and Order*, 2015 WL 5920207, at *2–3. Specifically, Judge Orenstein cited to the FBI's proposal to expand CALEA in 2009; congres-

In dicta, Judge Orenstein further noted that even if relief was available under the Act as a matter of law, the requested relief would be unduly burdensome to Apple under the rationale of *New York Telephone Co.*[158] Judge Orenstein primarily based this conclusion on the view that Apple was too far removed from the underlying investigation to be permissibly compelled to assist in execution of the warrant, and that the assistance order in this context would be inequitable for a number of reasons.[159] Furthermore, Judge Orenstein concluded that the government failed to establish that Apple's assistance in bypassing the lock screen was an absolute necessity, due to seemingly conflicting statements it had made in relation to the availability of third-party technologies and hacking tools.[160]

sional hearings occurring as far back as 2011 and as recently as July 2015 in which law enforcement officials had called for legislation on the matter; and the submission of three separate bills in 2015, each of which would preclude the government from forcing assistance from Apple. *See In re Apple, Inc.*, 149 F. Supp. 3d at 363 n.25.

[158] *See In re Apple, Inc.*, 149 F. Supp. 3d at 363–64.

[159] *See id.* (citing United States v. N.Y. Tel. Co., 434 U.S. 159, 172 174 (1977)). Specifically, Judge Orenstein noted that the record was replete with anything suggesting that Apple should be subject to greater regulation than any other business, and it does have a cognizable interest in choosing to design its products with uncompromising data security and declining to make an exception for the government. *See id.* at 369–70, 369 n.34. Judge Orenstein distinguished Apple from the telephone company in *New York Telephone Co.* in noting that Apple is not a highly regulated public utility, and it has no ownership interest in the phone, software, or anything else believed to have been used in connection with a criminal enterprise. *See id.* at 363–66. Additionally, Judge Orenstein determined that bypassing the lock-screen of a phone is not something Apple would normally do in the conduct of its own business, and due to its general initiative to be a leader in consumer data security, assistance could threaten its relationship with its consumers. *See id.* at 369. Thus, the situation was distinguishable from that in *New York Telephone Co. Id.* Similarly, Judge Orenstein noted that the burden on Apple would go well beyond the financial costs of diverting resources away from business operations, and would pose an irreconcilable threat to Apple's autonomy. *See id.* at 369–71.

[160] *See id.* at 373–75. Judge Orenstein was primarily concerned with the testimony of a U.S. Department of Homeland Security ("DHS") expert from another case, in which the expert indicated that the DHS was in possession of technology that would allow its forensic technicians to override the passcode of some iPhones and extract the phone's data. *See id.* (citing United States v. Djibo, 151 F. Supp. 3d 297, 304 (E.D.N.Y. 2015)). The government further noted that in this case, it could not risk using the forensic tool at issue to try to guess the password, because ten unsuccessful attempts may erase all of the phone's data; and even if that feature had not been enabled, the government may be unable to bypass a strong password before trial. *See id.* at 374. Additionally, the government indicated that the owner of the phone, the criminally charged in the underlying matter, had asserted that he forgot the password for the phone. *See id.* at 366 n.31. It further noted that even if he was not being truthful, to compel him to enter the password would raise significant Fifth Amendment issues, which could lead to a suppression of any evidence gathered from the phone. *See id.* Finally, the technique necessary for bypassing the phone without risking permanent loss of the data subject to the search warrant requires authentication from Apple servers, and can only be performed at Apple's facilities in Cupertino, California. *See In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 32–33, 63–64 ("We agree with the government that the system requires Apple authentication.").

B. Judge Orenstein Sets the Tone for the Encryption Debate in the Courts

Prior to Judge Orenstein's decision, Apple conceded that it has the ability to extract certain categories of unencrypted data from password protected devices running iOS 7 or earlier, but would not be able to do so on devices running on iOS 8 or higher.[161] It further argued that an order to perform this service would be unduly burdensome if extrapolated to a significant scale, but conceded that performing such service on one device would not impose any immediate financial or resource-based burden on the company.[162] At oral arguments, the government indicated that since 2008, Apple had received and complied with at least seventy court orders requiring technical assistance pursuant to the All Writs Act.[163] Apple indicated that it had purposefully taken itself out of a position to provide such assistance by developing iOS 8.[164] According to Apple, it was now asserting its first challenge because it no longer believed that the All Writs Act provided the authority the government had long claimed.[165]

Between October 2015 and February 2016, at least nine additional All Writs orders were issued by federal courts across the country directing Apple to assist the government to bypass the passcodes of a dozen iPhones running on a variety of iOS versions, all pursuant to the All Writs Act.[166] Notably, in one such preliminary order involving an iOS 9 that was later

[161] Apple Inc.'s Response to Court's October 9, 2015 Memorandum and Order at 3, *In re Apple, Inc.*, 149 F. Supp. 3d (E.D.N.Y. 2016) (No. 1:15-mc-01902) [hereinafter *Apple Inc.'s Response*] (noting that it would not have the ability to extract email, calendar entries, or any third-party app data).

[162] *See id.* at 3–4 (arguing that the burden would include: (1) allocation of man hours; (2) possibly requiring the Apple engineer who performed services to testify at a subsequent trial; and (3) a threat to the "trust between Apple and its customers [that could] substantially tarnish the Apple brand" (alteration in original)).

[163] *In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 8–9. This estimate was based on an initial internal survey, "an ongoing query of government prosecutors around the country." *Id.* According to Apple's privacy policy, it did have a practice of complying with such orders. *See id.* at 12. Attorneys from the ACLU, in its December 10, 2015 Freedom of Information Act Request, speculated that the vast majority of these seventy orders had been filed under seal, as they could not locate them on the federal dockets. Freedom of Information Act Request from Esha Bhandari, American Civil Liberties Union Foundation, to FOIA/PA Referral Unit at 5 (Dec. 10, 2015) [hereinafter *FOIA Request*], https://www.aclu.org/legal-document/foia-request-all-writs-act [https://web.archive.org/web/20160728235607/https://www.aclu.org/legal-document/foia-request-all-writs-act]. When asked by the court, why it was now challenging the type of order that it had regularly complied with in the past, Apple replied that it "does not want to be in the business of being a mechanism by which customer data is disclosed." *See In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 62.

[164] *See In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 58.

[165] *See id.* at 59–62.

[166] *See In re Apple, Inc.*, 149 F. Supp. 3d at 348; Letter in Response to Court's February 16, 2016 Order by Apple Inc. at 1–2, *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-01902).

withdrawn, a magistrate judge in the U.S. District Court for the Central District of California went as far as directing Apple to *create* and load Apple-signed software onto the target phone to enable the government to circumvent the data-wiping protocol and access the phone's data with the help of forensic tools.[167] Many quickly voiced opposition to the order, arguing that forcing Apple to write software unwillingly constitutes compelled speech, in violation of the First Amendment.[168] *In re Apple, Inc.* represents the first case in which a decision has been entered regarding the propriety of the All Writs Act's authority for compelling technical assistance of this type.[169] It remains to be seen whether the other courts will follow Judge Orenstein's lead and hold the Act inapplicable as a matter of law; withhold issuance on the grounds of burdensomeness; or grant the relief requested and order Apple to provide technical assistance.[170]

IV. THE LEGACY OF *IN RE APPLE, INC.* AND POTENTIAL LEGISLATIVE SOLUTIONS TO THE DEVICE-ENCRYPTION PROBLEM

Despite Magistrate Judge James Orenstein's decision in *In re Order Requiring Apple, Inc. Assist in Execution of Search Warrant* ("*In re Apple, Inc.*"), the All Writs Act is available as a matter of law to order third parties to provide decryption assistance.[171] The Act's availability, however, is lim-

[167] *See In re* Apple iPhone Seized During the Execution of Search Warrant on Black Lexus IS300 (*The San Bernardino Shooter Case*), No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016); Government's Ex Parte Application for Order Compelling Apple, Inc. to Assist Agents in Search at 2, *The San Bernardino Shooter Case*, No. ED 15-0451M, 2016 WL 680288 (C.D. Cal. Feb., 16, 2016) [hereinafter *San Bernardino Order Application*]; *see supra* note 15 and accompanying text (discussing the preliminary order issued in the *The San Bernardino Shooter Case* that would have required Apple to create and load a software update onto the target device to disable the iPhone's auto-erase function, and the government's subsequent withdrawal of its application due to a newly discovered alternative method for accessing the iPhone learned from a private third party).

[168] *See* Brief of Amici Curiae Electronic Frontier Foundation et al. at 4, 7–14, *The San Bernardino Shooter Case*, 2016 WL 618401 (C.D. Cal. Mar. 22, 2016) [hereinafter *San Bernardino Amicus Brief*], *available at* https://www.eff.org/files/2016/03/03/16cm10sp_eff_apple_v_fbi_amicus_court_stamped.pdf [https://perma.cc/8972-NQRL] (arguing that ordering Apple to write code according to government specifications is akin to unconstitutional compelled speech, because it is essentially forcing Apple to express itself in conflict with its stated beliefs).

[169] *See In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 55, 62.

[170] *See id.* at 62; Devlin Barrett, *Justice Department Seeks to Force Apple to Extract Data From About 12 Other iPhones*, WALL STREET J. (Feb. 23, 2016, 12:39 PM), http://www.wsj.com/articles/justice-department-seeks-to-force-apple-to-extract-data-from-about-12-other-iphones-1456202213 [https://perma.cc/6PM5-GAN8].

[171] *See, e.g.*, United States v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977); Ass'n for Retarded Citizens of Conn., Inc. v. Thorne, 30 F.3d 367, 370 (2d Cir. 1994); Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979).

ited to situations where such assistance will not be overly burdensome.[172] Thus, a less ephemeral solution will be needed to preserve the integrity of the warrant process; a responsibility that lies in the hands of Congress.[173] This Part argues that Judge Orenstein's principle holding in *In re Apple, Inc.* was incorrect and the product of improper statutory construction, however, obtaining assistance orders under the All Writs Act is not a viable solution to Going Dark in the long term.[174] The All Writs Act does authorize decryption-assistance orders as long as they are issued in conjunction with a device search warrant.[175] Application of the Act in this context comports with prior precedent, because full-disk, device encryption sits within a statutory gap that has only recently emerged and, in some instances, there is no feasible way to execute a warrant on an encrypted device without Apple's assistance.[176]

Section A of this Part argues that Judge Orenstein improperly construed the "usages and principles" provision of the Act; that there is no comprehensive statutory scheme that precludes the Act's use in this context; and that the Act does generally authorize decryption assistance orders.[177] Section B argues that, despite the Act's present applicability, using the Act to compel Apple to unlock iPhones running on iOS 8 or higher will eventually be unavailable due to judicial restraint, because of the undue burden those orders are likely to impose.[178] Section C argues that, by stripping the government of its reliance on the Act for unlocking iPhones, such judicial rulings should invigorate the push for legislative solutions to the Going Dark problem.[179] It will further offer an amendment to the Communication Assistance to Law Enforcement Act ("CALEA") that would effectively extend compliance requirements to device manufacturers as one possible solution.[180]

[172] *See N.Y. Tel. Co.*, 434 U.S. at 172 ("[T]he power of federal courts to impose duties upon third parties is not without limits, unreasonable burdens may not be imposed.").

[173] *See* Corn, *supra* note 10, at 1437, 1444–47, 1455 (advocating for Congress to require any manufacturer or distributor of communications and storage technologies to build in a "split-key" mechanism to allow for lawful government surveillance and searches of stored data).

[174] *See infra* notes 181–205 and accompanying text.

[175] *See, e.g.*, *N.Y. Tel. Co.*, 434 U.S. at 174; *Thorne*, 30 F.3d at 370; *Hutton*, 608 F.2d at 1289.

[176] *See N.Y. Tel. Co.*, 434 U.S. at 165–67; *In re* Application of U.S. for Order Authorizing Disclosure of Location Info. (*In re Application for Location Info. (D. Md.)*), 849 F. Supp. 2d 526, 580 (D. Md. 2011); Sousa, *supra* note 93, at 113–14; Portnoi, *supra* note 100, at 299.

[177] *See infra* notes 181–205 and accompanying text.

[178] *See infra* notes 206–211 and accompanying text.

[179] *See infra* notes 212–222 and accompanying text.

[180] *See infra* notes 212–222 and accompanying text.

A. Applesauce: A Questionable Construction in In re Apple, Inc.

To reach the court's principle holding in *In re Apple, Inc.*, Judge Orenstein first constructed the "usages and principles" provision to allow only orders that are consistent with how the law is developed, implemented, and interpreted.[181] This construction, however, was necessarily improper; the "usages and principle" provision has already been constructed by the U.S. Supreme Court to have a different meaning.[182] The Court has long understood the Act's gap-filling function as conferring authority to federal courts to enlarge the effect of their process through fashioning orders as the need presents itself.[183] Moreover, the Court has construed the "usages and principles" provision as limiting the procedural tools available under the Act to only orders that would (1) not be unconstitutional under the circumstances; (2) not be prohibited by any statute; and (3) not be prohibited by any common law principle.[184] Thus, an order that may raise separation of powers concerns or call-to-mind certain statutes covering similar matters, would still be "agreeable" under that alternative construction as long as it was not completely offensive to the doctrine or statutorily prohibited.[185] Under

[181] *See In re* Order Requiring Apple, Inc. Assist in Execution of Search Warrant (*In re Apple, Inc.*), 149 F. Supp. 3d 341, 349–54, 357–59, 363–64 (E.D.N.Y. 2016). The court did this after concluding that "[f]ederal case law offer[ed] little if any guidance." *Id.* at 353 (alteration in original). Under that construction, the court then considered whether an All Writs order in this context would be consistent with the statute's gap-filling function against the backdrop of the "surrounding body of pertinent laws." *See id.* at 359.

[182] *See* Kerr, *supra* note 149; *see also* Riggs v. Johnson, 73 U.S. (6 Wall.) 166, 182, 190 (1867) (discussing mandamus, but noting that writs may only be issued "in *subordination to* fixed principles of law," such as comity and agreeable to the usages of law, which includes the law of the several States in addition to common law (emphasis added)); United States v. Halstead, 23 U.S. (10 Wheat.) 51, 55–60 (1825) (interpreting the usages and principles provision as giving federal courts power to "mould their process, as to meet whatever changes might take place," and concluding that courts are authorized to alter their process and enlarge the effect of its operation); United States v. Perry, 360 F.3d 519, 533 (6th Cir. 2004) (noting that the "usages and principles" provision of the All Writs Act prohibits a subsequent order from issuing that is either unconstitutional, or in *violation* of some other statutory provision (emphasis added)).

[183] *See Halstead*, 23 U.S. (10 Wheat) at 55–60; *see also N.Y. Tel. Co.*, 434 U.S. at 173 ("[T]hese supplemental powers are not limited to those situations where it is 'necessary' to issue the writ or order 'in the sense that the court could not otherwise physically discharge its appellate duties.'" (quoting Adams v. U.S. *ex rel.* McCann, 317 U.S. 269, 273 (1942))); *Riggs*, 73 U.S. (6 Wall.) at 182, 190.

[184] *See Riggs*, 73 U.S. (6 Wall.) at 182, 190; *Halstead*, 23 U.S. (10 Wheat.) at 55–60; *Perry*, 360 F.3d at 533; *In re Apple, Inc.*, 149 F. Supp. 3d at 357–58; Kerr, *supra* note 149. This alternative construction of the provision, which can be read as limiting orders under the Act to those that are "consistent with the law," has more precedential support than Judge Orenstein's, although he explicitly rejected the former. *See Halstead*, 23 U.S. (10 Wheat.) at 60–61; *N.Y. Tel. Co.*, 434 U.S. at 173; *Perry*, 360 F.3d at 533; *In re Apple, Inc.*, 149 F. Supp. 3d at 357–58; Kerr, *supra* note 149.

[185] *See Riggs*, 73 U.S. (6 Wall.) at 182, 190; *Halstead*, 23 U.S. (10 Wheat.) at 55–60; *Perry*, 360 F.3d at 533; *In re Apple, Inc.*, 149 F. Supp. 3d at 357–58; Kerr, *supra* note 149. Issuing such an order could *threaten* the separation of powers without offending it, because if Congress disap-

Judge Orenstein's construction, however, such an order would not be agreeable to "usages and principles" because it could be deemed inconsistent with the way laws are developed, implemented, and interpreted.[186] The former construction has precedent, whereas the later has none.[187] Decryption-assistance orders, when sought to help execute a warrant, are consistent with that former construction because they violate no constitutional provision, statute, or common law principle.[188]

For example, CALEA does not apply to password encrypted devices and the underlying data at rest, because it is explicitly limited to the interception of real-time communications and call-identifying information transmitted by telecommunications carriers.[189] There may be other piecemeal legislation that could conceivably cover decryption-assistance orders if amended, such as the Stored Communications Act ("SCA"), but currently nothing specifically addresses the propriety of obtaining data at rest from a

proves of the judiciaries' actions it is within its power to impose corrective legislation. *See* Beers v. Haughton, 34 U.S. 329, 360 (1835) (8 Pet.) (approving the constitutionality of Congress's delegation to the courts); *Halstead*, 23 U.S. (10 Wheat.) at 60–62.

[186] *See In re Apple, Inc.*, 149 F. Supp. 3d at 360–63. Furthermore, an order that seems legislative in nature, and covers an area that has partially been considered by members of Congress, raises sufficient concerns of judicial usurpation of the legislative prerogative to support the view that issuing that order would be inconsistent with the manner in which laws are developed, implemented, and interpreted. *See id.*

[187] *See Halstead*, 23 U.S. (10 Wheat.) at 60–61; *N.Y. Tel. Co.*, 434 U.S. at 173; *Perry*, 360 F.3d at 533; *Govt's District Court Brief*, *supra* note 65, at 29–31; Kerr, *supra* note 149.

[188] *See N.Y. Tel. Co.*, 434 U.S. at 172–73; *Perry*, 360 F.3d at 533; Kerr, *supra* note 149. The search of the phone in this case would comply with the Fourth Amendment because the government obtained a warrant. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014) (holding that a warrant is generally required to search a cellphone); *In re Apple, Inc.*, 149 F. Supp. 3d at 352–53. It is not apparent that ordering private citizens to provide assistance to law enforcement is offensive to common-law principles, as the Supreme Court rejected that notion in *United States v. New York Telephone Co. See N.Y. Tel. Co.*, 434 U.S. at 175 n. 24 (noting that private citizens have been called upon the state, in certain situations, to assist in the enforcement of justice since the days of Edward I).

[189] 47 U.S.C. § 1002 (2012); King, *supra* note 79, at 178; *see* United States v. Steiger 318 F.3d 1039, 1047 (11th Cir. 2003) (noting that the term "intercept" applies only to "acquisitions contemporaneous with transmission"); The Government's Reply at 22–23, *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-01902) [hereinafter *Govt's Reply Brief*]; Hibbard, *supra* note 76, at 374–75. Particularly, CALEA does not apply to information service providers like Apple, or to the type of physical assistance sought by the government in this case, and it confers no independent authority upon the federal courts to issue assistance orders. *See* 47 U.S.C. § 1002(a); *Govt's Reply Brief*, *supra*, at 22–23. Furthermore, even if Apple is considered an information service provider under the exemption provision, the exemption only pertains to the capability requirements. *See* 47 U.S.C. § 1002(a); *Govt's Reply Brief*, *supra*, at 22–23. Furthermore, the other third-party assistance statutes in the statutory scheme to which Judge Orenstein refers, all cover very specific types of governmental acquisitions, none of which can be reasonably construed as decidedly omitting compelled assistance in bypassing the lock-screen of an encrypted device. *See Govt's Reply Brief*, *supra*, at 22–23 nn.5–6; *see also* 18 U.S.C. § 2703(f)(1) (2012) (requiring assistance to government acquisition of electronically stored data in the providers possession).

smartphone beyond the typical warrant requirements.[190] Moreover, no provisions of CALEA or the SCA have been updated since 1996 and 2006, respectively.[191] The iPhone was not released until 2007, and it was not offered with full-disk encryption ("FDE") or remote-wiping capabilities until 2009.[192] Thus, the further development of FDE and data-wipe features since 2009 has created a clear statutory gap.[193] There was no substantial need to seek this type of conscripted assistance prior to those developments, because few data was actually being encrypted at first and passcodes could be bypassed via simple forensic tools.[194] For more securely encrypted phones, Apple regularly provided assistance to the authorities.[195] Therefore, the specific practical inabilities presented in *In re Apple, Inc.* were largely nonexistent until very recently, so it is difficult to see how they could have been explicitly omitted from legislation after being fully considered.[196]

Although some members of Congress have been aware of the Going Dark issue since at least 2011, congressional hearings prior to 2015 focused more predominantly on the difficulties of intercepting real-time data in motion, rather than those associated with obtaining data at rest from physical devices.[197] The difference is significant under the *United States v. New York Telephone Co.* framework, where the U.S. Supreme Court in 1977 explicitly rejected the argument that pen registers could only be obtained through the seemingly pertinent Wiretap Act or not at all, because that statute did not

[190] *See Govt's District Court Brief*, *supra* note 65, at 22–23. For example, the Stored Communications Act ("SCA") applies to electronic communications held by electronic communication services and remote computing services; not manufacturers, passcodes, or data at rest on a user's phone. *See* Garcia v. City of Laredo, 702 F.3d 788, 792 (5th Cir. 2012); Wilson, *supra* note 1, at 31–32; *see also* 18 U.S.C. § 2510(12) (2012) (defining electronic communications). Furthermore, the Wiretap Act and Pen Register statute, cited by the court, both pertain to real-time surveillance and interception, not data at rest. *See* 18 U.S.C. §§ 2518(4), 3124(a) (2012).

[191] *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 104–316, § 126(b), 110 Stat. 3840 (amended 1996); Stored Communications Act, Pub. L. No. 109–162, § 1171(a)(1), 119 Stat. 3123 (amended 2006).

[192] *See* Radia, *supra* note 2.

[193] Pell, *supra* note 72, at 538.

[194] *See San Bernardino Order Application*, *supra* note 167, at 4–8 (explaining that the government is unable to bypass the passcode of the phone on its own, because of newer security features, such as the auto-erase function after ten consecutive failed attempts and delays between failed attempts); Radia, *supra* note 2.

[195] *See Govt's District Court Brief*, *supra* note 65, at 4; *In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 12.

[196] *See Govt's District Court Brief*, *supra* note 65, at 26.

[197] *See* Going Dark Part I, *supra* note 80, at 14, 42; McCullagh, *supra* note 80. More recent hearings, conducted in July 2015 and February 2016, have explicitly addressed the issue of encrypted iPhones, but it is difficult to see how those very recent hearings provide support for the conclusion that the issue has been fully considered by Congress and declined to be adopted. *See generally Encryption Tightrope Hearing*, *supra* note 84 (discussing full-disk encryption by default on smartphones); Going Dark Part II—Yates & Comey Statement, *supra* note 81 (same).

specifically cover the type of information being sought—non-content communication.[198] A similar "near miss" has occurred in the case with encrypted data at rest on user devices, as no statute specifically covers the matter.[199] Despite the lack of coverage, Judge Orenstein concluded that Congress chose not to confer decryption-assistance authority after sufficiently considering it by citing congressional hearings, the FBI's draft of CALEA amendments in 2009, and recently proposed legislation as support.[200] Congressional hearings and proposed amendments should do nothing to effect the availability of the All Writs Act under established precedent.[201] The inability to execute smartphone search warrants due to rapidly evolving commercial encryption seems to be exactly the type of "statutory interstice" for which the Act's invocation has been reserved.[202] Furthermore, decryption-assistance orders are "agreeable to the usages and principles of law" because they are not precluded by any constitutional provision, current statute, or common law principle when issued in conjunction with a valid search

[198] *See N.Y. Tel. Co.*, 434 U.S. at 162–63, 165–67; *Govt's Reply Brief*, *supra* note 189, at 23; Comey, *supra* note 11 (explaining the technical and practical difference between data at rest and data in motion as both falling under the umbrella term of Going Dark). In its decision, the Court explicitly rejected the telephone company's assertion that pen traps could only be obtained under the Wiretap Act, which covered the interception of communications contents, because pen registers did not intercept "the contents" of communication. *N.Y. Tel. Co.*, 434 U.S. at 165–67; *see also* Wiretap Act of 1968, 18 U.S.C. §§ 2510–2521 (1968) (regulating wiretaps in domestic criminal investigations). Furthermore, the essence of the order was in many respects approved years later when the ECPA was enacted in 1986, which provided regulations for acquiring pen registers—defined as non-content information. *See In re* Application of U.S. for Order Authorizing (1) Installation and Use of Pen Register and Trap Device or Process (*In re Application of U.S. (S.D. Tex)*), 441 F. Supp. 2d 816, 818–19, 830–31 (S.D. Tex. 2006).

[199] *See N.Y. Tel. Co.*, 434 U.S. at 162–63, 165–67; *Govt's District Court Brief*, *supra* note 65, at 26.

[200] *See In re Apple, Inc.*, 149 F. Supp. 3d at 363. *See generally Encryption Tightrope Hearing*, *supra* note 84 (discussing full-disk encryption by default on smartphones); Going Dark Part II—Yates & Comey Statement, *supra* note 81 (same). The FBI amendments were never sent to any member of Congress, and the proposed bills from 2015 have not yet been voted on. *See In re Apple, Inc.*, 149 F. Supp. 3d at 363; *see also* Secure Data Act of 2015, S. 135, 114th Cong. (2015) (exempting mandates authorized under CALEA, 47 U.S.C. §§ 1001–1010 (2012)); Secure Data Act of 2015, H.R. 726, 114th Cong. (2015) (same).

[201] *See N.Y. Tel. Co.*, 434 U.S. at 165–67; *In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 580; Sousa, *supra* note 93, at 113–14; Portnoi, *supra* note 100, at 299; *see also* Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985) (holding the All Writs Act inapplicable where a "statute specifically addresses the particular issue at hand"); Zino Davidoff v. CVS, 571 F.3d 238, 243 (2d Cir. 2009) ("Congressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction."). The implication of the court's construction is that courts must continually look to the legislative record, including proposed bills, congressional hearings and news stories to determine the actual will of Congress. *See* Kerr, *supra* note 149.

[202] *See* Syngenta Crop Prot., Inc. v. Henson, 537 U.S. 28, 32 (2002) ("[T]he All Writs Act 'fills the interstices of federal judicial power when those gaps threaten to thwart the otherwise proper exercise of federal courts' jurisdiction.'" (quoting *Pa. Bureau of Corr.*, 474 U.S. at 41)).

warrant.[203] Finally, Apple itself had purposefully designed the auto-wipe feature for iOS 7 to thwart the only alternative means of accessing a locked iPhone available to the government.[204] Thus, sufficient exceptional circumstances are present to make a decryption-assistance order in this case necessary to preserve the integrity of the court's previously issued warrant.[205]

B. Apples-to-Apples: Different All Writs Analysis Depending on the Device's Operating System

Due to the discretionary nature of the authority under the All Writs Act, its availability in this context as a matter of law does not mean that orders should be issued in every case.[206] As the *In re Apple, Inc.* court noted in extensive dicta, the discretionary factors that have been interpreted out of *New York Telephone Co.*, should ultimately determine whether an All Writs order is necessary and not unduly burdensome.[207] Although the court in *In re Apple, Inc.* concluded that the requested order would be unduly burdensome given the facts, for a number of reasons, other courts could and have found differently under the same or similar circumstances.[208] It would be

[203] *See Perry*, 360 F.3d at 533; *see also In re* Order Requiring XXX, Inc. to Assist in Execution of Search Warrant by Unlocking Cellphone (*In re XXX, Inc.*), No. 14 Mag. 2258, 2014 WL 5510865, at *1–3 (S.D.N.Y. Oct. 31, 2014) (issuing All Writs Act order to compel device manufacturer to assist in bypassing the lockscreen of a smartphones).

[204] *See* APPLE, INC., *supra* note 41, at 11; *Govt's District Court Brief*, *supra* note 65, at 41.

[205] *See Pa. Bureau of Corr.*, 474 U.S. at 44; *In re Application for Location Info. (D. Md.)*, 849 F. Supp. 2d at 581. *Govt's District Court Brief*, *supra* note 65, at 41–42. Because of the auto-wipe feature, the only feasible means of accessing the phone is by providing the phone to Apple and having them bypass the passcode using their servers. *Govt's District Court Brief*, *supra* note 65, at 41–42. The method of extracting the data is proprietary, and there is no way for Apple to instruct the government to do it on its own. *See id.*

[206] *See N.Y. Tel. Co.*, 434 U.S. at 172 ("[T]he power of federal courts to impose duties upon third parties is not without limits, unreasonable burdens may not be imposed."); United States v. Mountain States Tel. & Tel. Co., 616 F.2d 1122, 1132–33 (9th Cir. 1980) (holding that a company whose cooperation in electronic surveillance is sought should be afforded reasonable notice and an opportunity to be heard prior to the entry of such an assistance order under the Act); *In re* Installation of a Pen Register or Touch-Tone Decoder & Terminating Trap (*In re Pen Register or Touch-Tone (3d Cir.)*), 610 F.2d 1148, 1157 (3d Cir. 1779) (same).

[207] *See In re Apple, Inc.*, 149 F. Supp. 3d at 363–64, 368, 374–75 (citing *N.Y. Tel. Co.*, 434 U.S. at 174 172). Judge Orenstein noted three factors to consider: (1) closeness to the underlying matter; (2) burdensomeness; and (3) necessity. *See id.* Previous courts have considered these factors in a variety of different forms, and have articulated additional ones as well, but they all can be considered to ultimately determine burdensomeness. *See, e.g.*, *Mountain States Tel.*, 616 F.2d at 1132–33; *see supra* note 142 and accompanying text (discussing the discretionary considerations to determine whether an order would be unduly burdensome).

[208] *See, e.g.*, *In re XXX, Inc.*, 2014 WL 5510865, at *1–3 (issuing an All Writs Act order to compel device manufacturer to assist in bypassing the lock screen of a smartphones); Orin Kerr, Opinion, *Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case: Part 2, the All Writs Act*, WASH. POST (Feb. 19, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/19/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-2-the-

much more difficult, however, to rectify the burdensomeness of an assistance order seeking access to a phone running iOS 8 or higher, because Apple would most likely have to develop new software or handover source code to the government in order to comply.[209] Aside from the potential First Amendment implications, such an order would present more than a minimal level of disruption to Apple's overall operations, as it would require more research and development than the mere physical labor required to assist with pre-iOS 8 devices.[210] 'It is well within the courts' authority to continue issuing decryption-assistance orders under the All Writs Act as long as the burden of compliance imposed on Apple remains relatively minimal.[211]

all-writs-act [https://perma.cc/255R-GBBL]. There have been at least seventy instances in which courts had issued All Writs orders against Apple in the past, but because many of them were most likely filed under seal, it is difficult to say what has and has not been considered by courts issuing these orders in the past. *In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 8–9; *FOIA Request*, *supra* note 163, at 5. To be sure, Apple had never challenged an order until it did so in this case. *See In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 62. The argument can be made, however, that Apple purposefully designed its encryption to prevent law enforcement from gaining access, it was at least partially marketed as such, so it could arguably be considered "not so far removed" from the underlying search warrant that it's effectively nullifying. *See Govt's District Court Brief*, *supra* note 65, at 32–36. Despite what the court determined regarding necessity, the government's ability to access a phone on its own *is* highly device-specific, and it would be a clear and potentially untenable risk to run a brute-force forensic attack on a phone running the auto-erase feature because that's specifically what it is designed to thwart by erasing all of the phone's data. *See id.* at 41–44.

[209] *See In re Apple, Inc.*, 149 F. Supp. 3d at 348, 372–74; *In re* Apple iPhone Seized During the Execution of Search Warrant on Black Lexus IS300 (*The San Bernardino Shooter Case*), No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016); Bill Kaski, *Apple vs. FBI Has Turned into King Kong vs. Godzilla*, TECHAERIS (Mar. 16, 2016), http://techaeris.com/2016/03/16/apple-vs-fbi-turned-into-king-kong-vs-godzilla [https://perma.cc/D5TV-7RS2].

[210] *See N.Y. Tel. Co.*, 434 U.S. at 174–75. *In re Pen Register or Touch-Tone (3d Cir.)*, 610 F.2d at 1155; *San Bernardino Amicus Brief*, *supra* note 168, at 4–14; Kerr, *supra* note 149.

[211] *See N.Y. Tel. Co.*, 434 U.S. at 172. According to estimates, iOS 8 and higher is currently running on 95% of Apple devices, and on at least four out of those twelve targeted devices at issue in the nine pending All Writs assistance orders across the federal jurisdictions. *See* Letter from Apple in Response to Court's February 16, 2016 Order at 2, *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-1902); Yoni Heisler, *As iOS9 Adoption Reached 79%, Most Android Users Are Still Running a Painfully Old OS*, YAHOO (Mar. 15, 2016, 10:56 AM), http://news.yahoo.com/ios-9-adoption-reaches-79-most-android-users-145625164.html [https://perma.cc/6L87-3LAP]. Up until recently, the government had seemingly been relying on authority under the All Writs Act to bypass locked pre-iOS 8 devices. *See In re Apple, Inc.*, Transcript of Oct. 26, 2015, *supra* note 14, at 66. If the All Writs Act becomes obsolete in this area due to the burden imposed by orders involving iOS 8-plus phones, the likely response by the government is to either push harder for back-door legislation or attempt to develop alternative methods of bypassing phones. *See id.*; van Hoboken & Rubinstein, *supra* note 50, at 528

C. Expand CALEA to Require Cellphone Manufacturers to Maintain Decryption Capabilities When Presented with a Search Warrant

One long-term solution to the device-encryption problem could be to amend and expand CALEA to cover smartphone manufacturers, by requiring telecommunications carriers to retain certain decryption capabilities for devices running on their networks.[212] For example, this could be done by adding a fifth capability requirement to § 1002(a) that mandates telecommunications carriers to ensure that wireless devices sold for use on their networks are amenable to search warrant executions.[213] This would be consistent with the congressional intent underlying the original enactment of CALEA because the mandate would only directly apply to telecomm carriers, and actual access would still be predicated on an independently obtained warrant.[214] It would only indirectly apply to smartphone manufacturers through § 1005, which requires manufacturers to cooperate with telecomm carriers' CALEA compliance efforts.[215] Moreover, this would not necessarily extend CALEA to include all electronic communication services, something that Congress explicitly rejected with the original bill, because an entity could remain excluded insofar as it provides "information

[212] *See* FINKLEA, *supra* note 6, at 7, 10–11.

[213] *See* 47 U.S.C. § 1002(a). For example, Verizon Wireless, a covered carrier under CALEA, sells iPhones on its website and in its stores for use on the Verizon network under the terms of service plans provided by Verizon. *See* Apple Smartphones, VERIZON WIRELESS, http://www.verizonwireless.com/smartphones/apple [https://perma.cc/ETN5-GYHP]. Apple is substantially engaged in manufacturing cellular devices, which it distributes through Verizon and other cellular network carriers, among other channels. *See* APPLE, INC., 2015 FORM 10-K, at 1, 9, 53 (FY 2015). Thus, Apple is most likely an "equipment manufacturer" for Verizon under the cooperation provision of § 1005, although the term is not defined in CALEA nor in Chapter 47 of the U.S. Code, and there has been little caselaw or administrative guidance that has discussed whether smartphones are to be considered "telecommunications transmission equipment." *See* FCC, Opinion Letter on CALEA Section 107(c) Extension Petition Deadline for Packet-Mode Commc'n Verizon Wireless, 19 FCC Rcd. 22544, 22547 (Nov. 16, 2004) [hereinafter FCC Opinion Letter] (noting that Motorola was an equipment manufacturer for Verizon for purposes of § 1005 and its obligation to comply with CALEA).

[214] *See* H.R. REP. NO. 103-827, pt. 1, at 18 (1994). Congress narrowed the scope of CALEA's compliance requirements to telecomm carriers, and explicitly excluded information services to accommodate privacy concerns and avoid wide-sweeping technological impediments. *See id.* at 18–19. CALEA's stated purpose, however, was to preserve the government's ability to intercept communications that use advanced technology. *See id.* at 9. Thus, the statutory scheme reflects a balancing of interests; for example, application of compliance was limited to common carriers because they were entities that law enforcement most regularly served with surveillance orders. *See id.* at 18. Congress noted that a broader approach that included all providers of electronic communication services would not be practical, nor would it be justified to meet any law enforcement need. *Id.* This rationale also presumed that other services could be wiretapped pursuant to court order, which they must cooperate with under existing law. *Id.*

[215] 47 U.S.C. § 1005. As it is currently written, requires manufacturers of telecomm transmission equipment, which ostensibly includes Apple, to make available such features or modifications necessary to allow covered carriers to comply with capability requirements under § 1002(a).

services."[216] Furthermore, § 1002(b)(2)'s encryption exemption would be amended to also cover equipment manufacturers.[217] This would exempt carriers and manufacturers from being responsible for decrypting communications and devices encrypted by a subscriber or customer, but would require decryption assistance if the encryption was provided by that carrier or manufacturer.[218]

With this solution, the government is only mandating access in the general sense, rather than a specific access point that may contain untenable privacy vulnerabilities.[219] Allowing the private industry to come up with the most viable solution on its own terms, rather than mandating a specific key system would still allow for innovation and competition in the cryptology field.[220] This notion of requiring private entities to maintain capabilities to

[216] *See* 47 U.S.C. § 1002(b)(2)(A); H.R. REP. NO. 103-827, at 18. As it is currently written, CALEA excludes "information services" from capability requirements. 47 U.S.C. § 1002(b)(2)(A). While Apple offers many information services, such as iTunes, it also engages in manufacturing and distributing iPhones that are sold to operate on wireless networks, and can reasonably be considered telecommunication transmission equipment. *See Govt's District Court Brief*, *supra* note 65, at 20; APPLE, INC., 2015 FORM 10-K, at 1 (FY 2015); *see also* FCC Opinion Letter, *supra* note 213, at 22547 (noting that Motorola was an equipment manufacturer for Verizon for purposes of § 1005 and its obligation to comply with CALEA). An amendment could be devised that would include a company as far as they provide services for a covered function, such as an equipment manufacturer, but would exclude that company as far as it was engaged in providing information services. *See supra* note 77 and accompanying text (discussing how "information services" should be read narrowly, so that entities are both capable of being excluded from CALEA insofar as they provide information services, but included insofar as they act as telecommunication carriers). The benefit of this narrow formulation would be that the extension would only encompass encrypted on physical devices. *See* FINKLEA, *supra* note 6, at 7, 10–11. Thus, other internet services would remain unaffected, and large-scale security vulnerabilities would be curtailed. *See id.*

[217] *See* 47 U.S.C. § 1002(b)(3).

[218] *See id.* This would be consistent with original congressional intent to avoid limitations on subscribers' rights to use encryption, but would preclude a device manufacturer like Apple from refusing to assist the government in decrypting software or hardware that it designed itself. *See* H.R. REP. NO. 103-827, at 18, 24.

[219] *See* H.R. REP. NO. 103-827, at 23; FINKLEA, *supra* note 6, at 10. This approach may be preferable to other potential legislative solutions, such as a Key Escrow or Key Disclosure type of statute. *See* Atwood, *supra* note 64, at 431–33 (discussing key escrow and key disclosure statutes as possible solutions to the encryption problem); Corn, *supra* note 10, 1444–50 (advocating for a new statutory framework that would require tech manufacturers to preserve copies of encryption keys for the devices and service that they produce; require individual encryption keys to be "split" into two or more pieces and retained by the manufacturer and a privacy rights organization; and arguing that such a statutory scheme could mirror that of CALEA); Swire & Ahmad, *supra* note 39, at 470 (arguing that any type of comprehensive encryption regulation could harm cybersecurity).

[220] *See* H.R. REP. NO. 103-827, at 23. Moreover, the amendment could be implemented over a four-year transition period to allow carriers and device manufacturers to develop means of compliance, as the original act did. *See* H.R. REP. NO. 103-827, at 16–18. One of the original purposes behind the statutory exemptions was to not interfere with the free market, and allow for innovation. *See* van Hoboken & Rubinstein, *supra* note 50, at 529. Under the scheme of this proposed

comply with court-ordered government searches is not a novel concept.[221] By narrowly tailoring the amendment to meet this new challenge posed by advanced encryption technology, and allowing the industry itself to determine the terms of compliance, the amendment would be fairly consistent with the original congressional intent.[222]

CONCLUSION

The debate over cellphone encryption should ultimately be settled through legislation. Until then, the judiciary should be empowered to use the All Writs Act to preserve its jurisdiction where it would not be unduly burdensome to compel assistance. The Going Dark issue may indeed pose as a serious, real-time impediment to the public safety in the reasonably foreseeable future, or continue to proliferate as a tangential threat by making it more difficult for law enforcement to investigate and prosecute criminals. But more significant is the threat that this type of uncompromising technology, which has the potential to directly nullify the warrant requirement in an ever-expanding context, poses to the viability of the American criminal justice system. The Supreme Court has repeatedly noted that the hallmark of the Fourth Amendment is reasonableness. Just as it is reasonable to require authorities to obtain lawful authorization prior to conducting a search, it should be reasonable to require access once that authorization is obtained.

JOHN L. POTAPCHUK

amendment, third-party app encryption services, as well as end-to-end Internet encryption services, such as e-mail, would not need to ensure decryption capability.

[221] *See* van Hoboken & Rubinstein, *supra* note 50, at 529.

[222] *See* H.R. REP. NO. 103-827, at 16, 18; *supra* note 218 and accompanying text (discussing the legislative intent underlying CALEA's original enactment in 1994).