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

Sarah Wilson[†]

ABSTRACT

In 2012, the FBI served a search warrant on Google when a suspect—a user of Google's phone services—refused to answer any questions about his cellphone, or provide the agents with the password to unlock it. The search warrant compelled Google to hand over the password information and other identifying information for the cellphone (account log-in, password reset, and manufacturer default code), which Google refused to do. Google's refusal implicates a host of issues regarding our current understanding of privacy and self-incrimination protections and concerns legal scholars with what will happen to these doctrines if the government can simply bypass an individual and obtain passwords from a third party. This Article only begins to scratch the surface of this complex debate by analyzing the extent to which the Fourth and Fifth Amendments protect individuals when the government forces third parties to hand over their passwords, and will illustrate why these amendments do not adequately protect individuals in these situations. With constantly evolving technology and almost daily reports of the government accessing electronic communications and communication records, the time is ripe for Congress to legislate the issue of the government compelling private information, such as passwords, from third parties.

---

† J.D., Northwestern University School of Law, 2014; B.A., International Relations Global Business, University of Southern California, 2008. I would like to thank the members of the *Berkeley Technology Law Journal*, Jason Marsico, and Karin Lee for their invaluable comments and edits in developing this article. Most importantly, I would like to thank Matt Hienton for his love, support, and encouragement.

TABLE OF CONTENTS

I. INTRODUCTION

"A legal battle is brewing between technology companies and the U.S. government over whether law-enforcement agents have the right to obtain

passwords[1] to crack into smartphones of suspects."[2] Less than two years ago, the government seized a cellphone of a parolee suspected of becoming a "telephone pimp," but was unable to access the contents of the locked phone because the parolee would not divulge the passcode and forensic technicians were unable to otherwise gain access.[3] Although the government had obtained the cellphone from the suspect, the suspect refused to allow the government "access to it or answer any further questions."[4] Without the Google email username and password, however, the government could not access the contents of the seized cellphone.[5] The government likely realized—based on precedent—that obtaining the password from the suspect would have been a fruitless effort under the Fifth Amendment, and one in which it did not care to rest its case.[6] However, stumped by the

1. A password is "a secret word or expression used by authorized persons to prove their right to access" or "a word or other string of characters, sometimes kept secret or confidential, that must be supplied by a user in order to gain full or partial access to a multiuser computer system or its data resources." *Password*, DICTIONARY.COM, http://dictionary.reference.com/browse/password/ (last visited Feb. 8, 2015). Unless otherwise stated, "passwords" will be used to describe any passwords, encryption keys, or other strings of numbers or text that are used to secure data on an electronic device.

2. Julia Angwin, *FBI vs. Google: The Battle to Unlock Phones*, WALL ST. J., Sept. 7, 2012, at B4. *See also* Cyrus Farivar, *Feds Want Apple's Help to Defeat Encrypted Phones, New Legal Case Shows*, ARS TECHNICA (Dec. 1, 2014, 9:00 AM), http://arstechnica.com/tech-policy/2014/12/feds-want-apples-help-to-defeat-encrypted-phones-new-legal-case-shows/ (explaining that the DOJ has invoked the All Writs Act to facilitate the unlocking of a phone and noting the concern from at least one legal commentator that the "government's application raises troubling questions about the extent to which it can force companies to break the products they sell"). In covering stories like these, recent news articles have fueled the idea that the U.S. government is compelling major internet companies to divulge users' stored passwords and encryption algorithms. *See, e.g.*, Declan McCullagh, *Feds Tell Web Firms to Turn Over User Account Passwords*, CNET (July 25, 2013, 11:26 AM), http://news.cnet.com/8301-13578_3-57595529-38/feds-tell-web-firms-to-turn-over-user-account-passwords/ (explaining that an internet industry source confirmed that he has seen the government ask for passwords and that they push back. Also, an employee at a large Silicon Valley company "confirmed that it received requests from the federal government for stored passwords.").

3. Angwin, *supra* note 2, at B4.

4. Affidavit for Search Warrant at 5, *In re* Search of Google Inc., No. 3:12-mj-00882-NLS (S.D. Cal. Mar. 9, 2012)

5. *Id.* at 7.

6. *See, e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010); *In re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *1, *4 (D. Vt. Feb. 19, 2009) (directing the defendant to provide an unencrypted version of his hard drive where the government's expert was unable to search a computer because of password-protection and where the subpoena had asked for "any passwords used or associated with the [laptop]"). It is worth noting that in *In re* Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009), the magistrate judge found that the act of producing the password was testimonial and privileged, and as a

"pattern lock" on the phone, and the prospect of causing a lock-out by repeated incorrect attempts at the password, the government sought a search warrant ordering Google to "provide . . . any and all means of gaining access, including login and password information, password reset, and/or manufacturer default code."[7] Thus, the government chose to bypass the suspect's potential Fifth Amendment claim by attempting to obtain the device's password from the suspect's cellphone manufacturer.[8] The government sidestepped this potential roadblock and in so doing raised an important question: what is left of digital self-incrimination protection when the government can circumvent the Fifth Amendment by obtaining personal passwords from a third party?

Although Google refused to unlock the phone or even turn over the requested information,[9] the implications of the government's request, combined with constant innovation and evolving technology, warrant a discussion and a call for an update to the laws to prevent such workarounds from occurring without an individual's consent. Moreover, the use of encryption, while just starting to take hold in the cellphone context, "is likely to reach into virtually every aspect of our lives."[10] Thus, Congress and the courts must carefully consider Americans' constitutional rights in deciding whether to allow government compulsion of passwords from users and from third-party providers.

This Article will focus on the current understanding of password protections in the digital age, will consider to what extent the Fourth and Fifth Amendments protect individuals when the government forces third parties to hand over their passwords, and will illustrate why these amendments do not adequately protect individuals in these situations. This

result, on appeal, the request for a password was revised to a request for an unencrypted version of the hard drive. *See Boucher II*, 2009 WL 424718, at *1.

7. Affidavit for Search Warrant, *supra* note 4, at 1, 7 ("A pattern lock is a modern type of password installed on electronic devices, typically cellular telephones. To unlock the device, a user must move a finger or stylus over the keypad touch screen in a precise pattern so as to trigger the previously coded un-locking mechanism. Entering repeated incorrect patterns will cause a lock-out, requiring a Google email login and password to override."); *see also* Angwin, *supra* note 2, at B4.

8. *See* Affidavit for Search Warrant, *supra* note 4.

9. *See* Search and Seizure Warrant at 2, *In re* Search of Google Inc., No. 3:12-mj-00882-NLS (S.D. Cal. Mar. 26, 2012) (noting that "no property was obtained as Google Legal refused to provide the requested information"); *see also* Angwin, *supra* note 2, at B4 (noting that Google's refusal was unusual and controversial and "indicates how murky the legal standards are for new technologies such as smartphones").

10. *Privacy in the Digital Age: Encryption and Mandatory Access: Hearing Before the Subcomm. on the Constitution, Federalism, & Prop. Rights of the Comm. on the Judiciary*, 105th Cong. 3 (1998) (statement of Sen. Russell D. Feingold), *available at* http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Article will first address, in Part II, the rapidly changing technology that warrants a dialogue about individuals' waning privacy protections. Next, in Parts III and IV, this Article will discuss the Fourth Amendment privacy protections afforded to technology, the role of the Fifth Amendment in protecting passwords compelled by the government, and the shortcomings of these amendments in protecting passwords from third-party disclosures.

By exploring traditional analyses of the Fourth and Fifth Amendments and considering their application when the government compels passwords or other data "locking" mechanisms from third parties, this Article will illustrate the new paradigm that individuals face in their potential loss of constitutional protections. Unlike most articles that address whether the Fifth Amendment prevents the government from forcing an *individual* to provide a password or encryption key to permit access to his or her digital files,[11] this Article explores the issues that arise when the government compels *third parties* to provide a password or encryption key. To adequately address this issue, Part V will consider the impact of the Electronic Communications Privacy Act ("ECPA") and specifically one subpart of it, the Stored Communications Act ("SCA"), when certain third parties are compelled to hand over user's information. Finally, in Part VI, this Article will focus on the differences between two groups of third parties—service providers[12] and employers—that could be approached for passwords and will detail why, despite the differences, service providers and employers should be treated similarly when forced to compel data, at least at the present time.[13] In addressing the two categories of third parties, Part VI will also detail potential solutions for combatting the compulsion of passwords from third parties and will explain why Congress should amend the ECPA to balance

11. *See, e.g.*, Susan W. Brenner, *Encryption, Smart Phones, and the Fifth Amendment*, 33 WHITTIER L. REV. 525, 527, 535 (2012); Joshua A. Engel, *Rethinking the Application of the Fifth Amendment to Passwords and Encryption in the Age of Cloud Computing*, 33 WHITTIER L. REV. 543, 556 (2012); John E. D. Larkin, *Compelled Production of Encrypted Data*, 14 VAND. J. ENT. & TECH. L. 253, 264–72 (2012); Marjorie A. Shields, Annotation, *Fifth Amendment Privilege Against Self-Incrimination as Applied to Compelled Disclosure of Password or Production of Otherwise Encrypted Electronically Stored Data*, 84 A.L.R. 6TH 251 (2013).

12. As used in this Article, "service providers" refers to phone manufacturers, email and telecom providers, and any third-party service where users store password-protected information.

13. It is possible that a time will come when "keystroke logging" policies become commonplace in the workplace and that employees know that their employers can make permanent records of the passwords they enter into employer-provided devices. Should this change take place, employees will no longer have a reasonable expectation of privacy in the passwords they type into an employer-owned device and, in such a case, employers should be treated differently from third-party service providers.

the needs of law enforcement with the privacy interests of users in this rapidly changing digital world.

II. HOW RAPIDLY CHANGING COMMUNICATIONS TECHNOLOGY COULD THREATEN INDIVIDUALS' PRIVACY RIGHTS

The first generation cellphone was, plainly, a mobile phone, albeit a heavy one that was considered a rich man's toy.[14] Similar to a landline, the cellphone was simply meant for talking. The cellphone of today is far more than that: it is a pocket-sized computer with email, texting, calling, GPS, and web-surfing capabilities.[15] In fact, some may even say that "the term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."[16] As the cellphone has evolved, so too has the number of Americans who own one. As of January 2014, 90% of American adults have a cellphone.[17] Some 63% of cellphone owners use their phones to access the internet, 52% exchange emails, and 50% download apps.[18] Over 80% of cellphone owners use their phones to send or receive text messages.[19] And 49% "get directions, recommendations, and other location-based information."[20] Thus, to a law enforcement agency, cellphone passwords "can be the key to unlocking a larger trove of information such as emails, texts, calls and address lists."[21]

---

14. Marguerite Reardon, *Cell Phone Industry Celebrates Its 25th Birthday*, CNET (Oct. 13, 2008, 1:52 PM), http://www.cnet.com/news/cell-phone-industry-celebrates-its-25th-birthday/.

15. *See, e.g.*, United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) ("A cell phone is similar to a personal computer that is carried on one's person . . . ."); Kristin Judge, *Protecting Your Mobile Phone: Password Lock and GPS Tracking Apps Can Help*, ANN ARBOR NEWS (Mar. 1, 2012, 10:00 AM), http://www.annarbor.com/lifestyles/protecting-your-mobile-phone-password-locks-and-gps-tracking-applications-can-help/ ("In the 90s, a cellular phone was just a phone. The phone of 2012 is now a pocket-sized computer. The information you have access to from your phone is a wonderful thing."); Arthur Pinkasovitch, *Cell Phone Evolution*, INVESTOPEDIA (Mar. 19, 2010), http://www.investopedia.com/financial-edge/0310/cell-phone-evolution.aspx (explaining that apps on modern cellphones "help users watch movies, choose restaurants, do online banking, provide medical reference material, trade stocks, lose weight, navigate directions, read barcodes and performs millions of other fun and useful features").

16. Riley v. California, 134 S. Ct. 2473, 2489 (2014).

17. *Mobile Technology Fact Sheet*, PEW RESEARCH CTR., http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited Jan. 3, 2015).

18. *Id.*

19. *Id.*

20. *Id.*

21. Angwin, *supra* note 2, at B4.

As cellphones and computers have become more sophisticated, users have been able to conceal the data stored within them with more complex and sophisticated methods. While users can create a password to "lock" the device, they can also further protect devices by using encryption,[22] "which requires a password or device . . . to decrypt the data into readable form."[23] With password or encryption protection, files, directories, and applications are protected from unauthorized access.[24] Moreover, with encryption, "[o]nly the person holding the password is able to gain access to the original plaintext."[25] While a number of smartphone apps have been available for some time now for "encrypting particular types of files, such as emails (i.e., NitroDesk TouchDown), voice calls (i.e., RedPhone), and text messages (i.e., Cypher),"[26] full-disk encryption for smartphones is a relatively new feature,[27] but one that is increasingly used.[28] Full-disk encryption is a way to convert

22. "Encryption is a process of translating a message, called the Plaintext, into an encoded message, called the Ciphertext. This is usually accomplished using a secret Encryption Key and a cryptographic Cipher. Two basic types of Encryption are commonly used: Symmetric Encryption, where a single secret key is used for both encryption and decryption [and] Asymmetric Encryption, where a pair of keys is used—one for Encryption and the other for Decryption." *Definition of Encryption*, HITACHI ID SYS. INC., http://hitachi-id.com/concepts/encryption.html (last visited Aug. 24, 2013).

23. 117 AM. JUR. TRIALS 193 § 5 (2012).

24. "Encryption holds the promise of providing all of us with the ability to protect data and communications from unlawful and unauthorized access, disclosure, and alteration." *Privacy in the Digital Age: Encryption and Mandatory Access: Hearing Before the Subcomm. on the Constitution, Federalism, & Prop. Rights of the Comm. on the Judiciary*, 105th Cong. 18 (1998) (prepared statement of Robert S. Litt, Principal Assoc. Deputy Att'y Gen.), *available at* http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf; *see also Encrypting Your Smartphone Data*, BLACKBERRY SECURITY FEATURE OVERVIEW, http://docs.blackberry.com/en/smartphone_users/deliverables/39933/1812723.jsp (last visited Aug. 16, 2013) ("When you turn on encryption in the security options, your smartphone encrypts data stored on your smartphone (for example, browser information, messages, tasks, and calendar entries), including data that your smartphone receives when it is locked. If potentially malicious users attempt to access your data directly from the internal smartphone hardware, they can't decrypt and read the data without knowing your smartphone password.").

25. Michael S. Mahoney, Comment, *Compelling the Production of Passwords: Government's Ability to Compel the Production of Passwords Necessary to the Discovery of Encrypted Evidence in Criminal Proceedings, Merely a Choice of Words*, 6 T.M. COOLEY J. PRAC. & CLINICAL L. 83, 89 (2003).

26. Ryan Radia, *Why You Should Always Encrypt Your Smartphone*, ARS TECHNICA (Jan. 16, 2011, 10:00 PM), http://arstechnica.com/gadgets/2011/01/why-you-should-always-encrypt-your-smartphone/2/.

27. *Id.* (noting that the iPhone 3GS, released in June 2009, marked Apple's "first serious attempt" at full-disk encryption—which allowed the phone to be wiped remotely in seconds—while Motorola has stated that at least two of its Android smartphones "will soon offer full encryption").

28. *See, e.g.*, Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST BLOG (Sept. 18, 2014), http://www.washingtonpost.com/blogs/

everything on a hard drive, including the operating system, into an unreadable form until the proper key (i.e., password) is entered.[29] And while privacy advocates are rightfully rejoicing over recent moves by Apple and Google to expand the use of encryption on smartphones, law enforcement fears a certain downside to encryption, specifically that it will become impossible to collect evidence from smartphones, even with a search warrant.[30] The FBI has reported that "encryption has been used to conceal criminal activity and thwart law enforcement efforts to collect critical evidence needed to solve serious and often violent criminal activities."[31] And while criminal activity may be fueling the government's request for third parties to fork over passcodes, information security concerns are causing phone manufacturers to create engineering solutions to remove backdoor access (an ability for manufacturers to unlock a device) to a phone's passcode, such that it will no longer be feasible for the manufacturers to respond to government warrants—unless the data is stored in the server's cloud.[32] This move has been questioned by some[33] and touted by others.[34]

---

the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/ ("The next generation of Google Android's operating system . . . will encrypt data by default."). One legal scholar in particular "believe[s] we will see an increased use of encryption and other data-protection measures that will make it increasingly difficult, if not impossible, for officers to access the contents of a smart phone or other digital device by bypassing minimal, if any, security measures." Brenner, *supra* note 11, at 533.

29. KAREN SCARFONE ET AL., GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES 3-1 to -2 (2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

30. Timberg, *supra* note 28.

31. *Privacy in the Digital Age: Encryption and Mandatory Access: Hearing Before the Subcomm. on the Constitution, Federalism, & Prop. Rights of the Comm. on the Judiciary*, 105th Cong. 4 (1998) (statement of Sen. Russell D. Feingold), *available at* http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

32. Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/business/technology/apple-will-no-longer-unlock-most-iphones-ipads-for-police-even-with-search-warrants/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html.

33. *See, e.g.*, Orin Kerr, *Apple's Dangerous Game*, WASH. POST (Sept. 19, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/ (finding "Apple's new design very troubling"). Although, Orin Kerr subsequently changed his view from "very troubled" to "need more information." Orin Kerr, *Apple's Dangerous Game, Part 2: The Strongest Counterargument*, WASH. POST (Sept. 22, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/22/apples-dangerous-game-part-2-the-strongest-counterargument/; *see also* Craig Timberg & Greg Miller, *FBI Blasts Apple, Google for Locking Police Out of Phones*, WASH. POST (Sept. 25, 2014), http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html ("FBI Director James B. Comey sharply criticized Apple and Google . . . for developing forms of smartphone encryption so secure that law enforcement officials cannot easily gain access to information stored on the devices.").

Although technology has changed, privacy rights should not. "At one point, [the Fourth and Fifth Amendment] together barred government from 'any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence'" against him.[35] Unfortunately the point in time where a compulsion was deemed to be an invasion of constitutional liberty and security, as embodied in the Fourth and Fifth Amendments,[36] was short-lived.[37] Americans should be protected against government intrusion into their passwords,[38] but, as this Article will illustrate, under current law, they are not.

III. THE FOURTH AMENDMENT & THE REASONABLE EXPECTATION OF PRIVACY

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[39] Its fundamental purpose is to "safeguard the privacy and security of individuals against arbitrary invasions by government officials."[40] In order to prove a violation of the Fourth Amendment, one must be able to demonstrate that a "search" occurred, i.e., that the government infringed upon an individual's legitimate expectation of privacy.[41] But, that expectation of privacy must be reasonable from both a subjective and objective point of view. The standard requires "first, that a person exhibited an actual or subjective expectation of privacy and second,

34. Julian Sanchez, *Old Technopanic in New iBottles*, CATO (Sept. 23, 2014, 5:17 PM), http://www.cato.org/blog/old-technopanic-new-ibottles (pointing out "excellent security reasons not to mandate backdoors" and asking us to think if encryption is "really any worse than a system of pay phones that allow criminals to communicate without leaving *any* record for police to sift through after the fact").

35. Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J.L. & TECH. 12, 24 (2011) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

36. Boyd v. United States, 116 U.S. 616, 630 (1886) ("The principles laid down in this opinion affect the very essence of constitutional liberty and security . . . they apply to all invasions on the part of the government and its employés of the sanctity of a man's home and the privacies of life.").

37. A little over thirty years after the Court found that the Fourth and Fifth Amendment protected individuals from government invasions, the Court began eroding this position in *Olmstead v. United States* by not finding police wiretapping to be an unreasonable search. 277 U.S. 438, 466 (1928).

38. Leslie Harris & Grover Norquist, *Protecting Our Privacy in the Digital Age*, THE HILL'S CONG. BLOG (June 19, 2013, 12:00 PM), http://thehill.com/blogs/congress-blog/civil-rights/305735-protecting-our-privacy-in-the-digital-age/.

39. U.S. CONST. amend. IV.

40. Camara v. San Francisco Mun. Ct., 387 U.S. 523, 528 (1967).

41. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128 (1978); 68 AM. JUR. 2D *Searches & Seizures* § 6 (2014).

that the expectation be one that society is prepared to recognize as reasonable."[42] If this standard is met, the government may not compel this information from an individual or a third party without first obtaining a warrant based on probable cause.[43]

A. REASONABLE EXPECTATION OF PRIVACY IN THE CONTEXT OF EVOLVING TECHNOLOGY

Courts and government officials alike have struggled to apply the Fourth Amendment expectation of privacy test to electronic devices and technology (such as computers, cellphones, emails, the internet, and encryption), and have yet to create a clear standard to be applied in the context of evolving technology.[44] But, "the Fourth Amendment must keep pace with the inexorable march of technological process, or its guarantees will wither and perish."[45]

(1) Computers. The Fourth Amendment protection afforded to computers is not well defined, and is often determined by the circumstances surrounding the computer files and the extent to which the files are protected. Courts, however, tend to start with the underlying assumption that individuals have a reasonable expectation of privacy in files stored on their hard drives, as closed computer files resemble closed containers.[46] The expectation of privacy tends to disappear, though, when: (1) the search of a computer is conducted at the U.S. border;[47] (2) the search is on an employer-owned computer where the employer gave notice of its policy to monitor computer use;[48] (3) when an individual's computer files are accessible to

42. 117 AM. JUR. TRIALS 193 § 2 (2012); *see also* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); United States v. Ward, 561 F.3d 414, 414 (5th Cir. 2009).

43. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

44. *See* 3A CHARLES ALAN WRIGHT ET AL., PRACTICE & PROCEDURE § 663 (4th ed. 2013) ("One of the most difficult questions raised by the reasonable-expectation-of-privacy test for defining searches is how it applies in a world of digital communications.").

45. United States v. Warshak, 631 F.3d at 285.

46. *See* United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (holding that the "Fourth Amendment protection of closed computer files and hard drives is similar to the protection it affords a person's closed containers and closed personal effects"); *see also* United States v. Crist, 627 F. Supp. 2d 575, 586 (M.D. Pa. 2008); United States v. Knoll, 16 F.3d 1313, 1320 (2d Cir. 1994) (holding that "[i]f the files were closed and their contents not apparent from the exterior, the reasonable expectation of privacy continued so long as the files had not been searched before contact with the government occurred").

47. *See* United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008) (confirming that "searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment").

48. *See* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

others via a peer-to-peer file sharing software;[49] or (4) because the computer is shared with a third party[50] (unless separate passwords and accounts are set-up between the parties[51]).

(2) Cellphones. There is little dispute that an individual has a subjective expectation of privacy in their cellphone because of the wealth of information stored on it.[52] After all, "the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy."[53] However, courts have long questioned whether there is an objective expectation of privacy in a cellphone. Although courts have been split on this question, the Supreme Court recently stated in dicta that "a warrant is generally required before [searching a cellphone]."[54] However the case itself and the Court's holding was focused on requiring a warrant "when a cell phone is seized incident to arrest."[55] Thus, the law is not yet settled and it remains to be seen to what extent other courts will follow the general principle espoused by the Supreme Court. And, following this monumental case in favor of increased privacy protections of cellphones, it is unclear what will come of the rulings where courts have allowed government officials to search an individual's cellphone without a warrant, such as when the

49. *See* United States v. Stults, 575 F.3d 834, 843 (8th Cir. 2009) (holding that an individual had no reasonable expectation of privacy in files retrieved from his personal computer because he made his files accessible to others through file sharing); *see also* United States v. Conner, 521 Fed. App'x 493, 494 (6th Cir. 2013) (explaining that the "ability to download a file directly from another user's personal computer is known as 'peer-to-peer' file sharing"). For more information about peer-to-peer file sharing, see *What You Need to Know About Peer-to-Peer File Sharing*, ZONEALARM (June 4, 2014), http://www.zonealarm.com/blog/2014/06/what-you-need-to-know-about-peer-to-peer-file-sharing/ (explaining that peer-to-peer file sharing "is the process of sharing and transferring digital files from one computer to another").

50. *See* United States v. Matlock*,* 415 U.S. 164, 171 n.7 (1974) (holding that mutual use of property gives the co-inhabitants the right to permit inspection of shared common property).

51. *See* Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (finding that although a shared user of the computer in question "had authority to consent to a general search of the computer," and the joint hard drive, her authority did not extend to the other user's password-protected files).

52. *See, e.g.*, United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (recognizing that "cell phones contain a wealth of private information," and, as a result, individuals have a "reasonable expectation of privacy" in them); State v. Smith, 920 N.E.2d 949, 954–55 (Ohio 2009) (recognizing that "a person has a high expectation of privacy in a cell phone's contents" and therefore a subjective expectation of privacy in cellphones because "modern cell phones are capable of storing a wealth of digitized information").

53. United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013).

54. Riley v. California, 143 S. Ct. 2473, 2493 (2014).

55. *Id.* at 2493–94 (2014) (leaving open the possibility that "other case-specific exceptions may still justify a warrantless search of a particular phone").

government was seeking non-content data or attempting to preserve destructible data.[56] However, it will be hard to ignore the Supreme Court's finding that "[m]odern cell phones . . . implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[57] In fact, it may be that more courts will follow in step with others that have ruled that the government cannot search an individual's cellphone without a warrant,[58] such that individuals will soon hold an explicit objective expectation of privacy in cellphones. But, perhaps with such ambiguity, it will be left to the states to take action legislatively to expressly state that a search warrant is needed to seek information on an electronic device.[59]

(3) Emails. Although government entities can utilize the Stored Communications Act—an Act that addresses voluntary and compelled disclosure of information by third parties—"to compel a service provider to disclose the contents of [electronic] communications,"[60] most courts recognize, nevertheless, that there is both a subjective and objective expectation of privacy in the contents of emails and thus afforded emails Fourth Amendment protection.[61] Emails often contain the contents of an

56. *See, e.g.*, *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013) (relying on the third-party doctrine to compel historical location data from cellphone service providers without a warrant, and implying that this data was not subject to a reasonable expectation of privacy); United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009).

57. *Riley*, 143 S. Ct. at 2489.

58. *See, e.g.*, United States v. Wurie, 728 F.3d 1, 14 (1st Cir. 2013) (internal citation omitted), *aff'd sub nom.* Riley v. California, 134 S. Ct. 2473 (2014); United States v. Zavala, 541 F.3d 562, 576–77 (5th Cir. 2008) (holding that individuals have a reasonable expectation of privacy regarding the information in a cellphone and the search of a suspect's cellphone without a warrant violated the Fourth Amendment); Smallwood v. State, 113 So. 3d 724, 735 (Fla. 2013) (holding that once the electronic, computer-like phone was removed from the arrestee, the officer was "constitutionally required to obtain a warrant before searching the contents of, and the data in" the cellphone); State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) (finding that "because a person has a high expectation of privacy in a cell phone's contents, police must then obtain a warrant before intruding into the phone's contents"). But, even in a case decided after *Riley*, a court has held that Fourth Amendment protections do not apply to cell site location information. *See* United States v. Banks, 2014 U.S. Dist. LEXIS 128906 (D. Kan. Sept. 15, 2014).

59. *See, e.g.*, MONT. CODE ANN. § 46-5-110 (2013) (noting that "a government entity may not obtain the location information of an electronic device without a search warrant" unless authorized by the user, there is a life-threatening situation, or the user reports a call for emergency services or that the device has been stolen).

60. Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008).

61. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010); *In re* Applications for Search Warrants for Info. Associated with Target Email Address, No. 12-MJ-8119-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (holding that "an individual has a reasonable expectation of privacy in emails" and that the Fourth Amendment protections apply to email); *In re* Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., No. 14-228

individual's business and personal life, and it is highly unlikely that given their often sensitive and sometimes damning contents, individuals "expect[] them to be made public, for people seldom unfurl their dirty laundry in plain view."[62] Like the telephone user, an email user is "entitled to assume that the words he utters into [a device] will not be broadcast to the world."[63] And given the fundamental similarities between email and other traditional forms of communication, like the telephone and the letter, it would "defy common sense to afford emails lesser Fourth Amendment protection."[64] Thus, society is prepared to recognize an expectation of privacy in emails.

(4) The internet and encryption. Recently, the IRS "argued that anyone who used the internet had no reasonable expectation of privacy against governmental intrusion."[65] However, some legal scholars have argued that an individual should rightfully claim a reasonable expectation of privacy in the contents of internet pages and cloud computing when the individual safeguards those contents through reasonable concealment efforts, such as password protection and encryption.[66]

(JMF), 2014 WL 945563, at *8 (D.D.C. Mar. 7, 2014) (noting the "obvious expectation of privacy e-mail account holders have in their communications"); United States v. DiTomasso, No. 14-CR-160 SAS, 2014 WL 5462467, at *9 (S.D.N.Y. Oct. 28, 2014) (holding that defendant had a reasonable expectation of privacy in e-mails but waived this Fourth Amendment protection by agreeing to AOL's terms of service).

62. *Warshak*, 631 F.3d at 284.

63. Katz v. United States, 389 U.S. 347, 352 (1967).

64. *Warshak*, 631 F.3d at 285–86.

65. Ray Bishop, *Protecting Our Privacy in the Digital Age*, CRITICAL DECISIONS (June 21, 2013), http://critical-decisions.com/Index/2013/06/21/protecting-our-privacy-in-the-digital-age/. The 2009 search warrant handbook from the IRS Criminal Tax Division's Office of Chief Counsel asserts that "the Fourth Amendment does not protect communications held in electronic storage, such as email messages stored on a server, because internet users do not have a reasonable expectation of privacy in such communications." IRS OFFICE OF CHIEF COUNSEL CRIMINAL TAX DIVISION, SEARCH WARRANT HANDBOOK 59 (2009), *available at* https://www.aclu.org/national-security/search-warrant-handbook/. *See also* Nathan Freed Wessler, *New Documents Suggest IRS Reads Emails Without a Warrant*, AM. CIVIL LIBERTIES UNION (Apr. 10, 2013), https://www.aclu.org/blog/technology-and-liberty-national-security/new-documents-suggest-irs-reads-emails-without-warrant/ (claiming that "IRS Criminal Tax Division has long taken the position that the IRS can read your emails without a warrant—a practice that one appeals court has said violates the Fourth Amendment"). *But see* Harris & Norquist, *supra* note 38 (noting that when this policy was brought to light, the IRS backed off and said that "it would obtain a search warrant in all cases when seeking from an Internet service provider the content of email communications stored on behalf of customers").

66. *See, e.g.*, WAYNE R. LAFAVE, 1 SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(f) (4th ed. 2004); David A. Couillard, Note*, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2232 (2009).

In 1998, before encryption and passwords became the status quo on all electronic devices, Senator Russ Feingold remarked that "the fundamental right to privacy . . . will be at least somewhat sacrificed"[67] if an encryption user is denied the right to keep his personal information completely private by the inability to purchase non-recoverable encryption (i.e., encryption that can only be broken by the user's password, not by a backdoor). But, it is unclear how a recoverable encryption key or password (a backup or "backdoor" decryption capability) affects a user's reasonable expectation of privacy. If a third party is compelled to hold another key or backdoor to a cellphone's password, the user's password may not be protected by the Fourth Amendment, as one can hardly find a reasonable expectation of privacy in recoverable encryption.[68] However, with non-recoverable encryption, users are able to keep their information completely confidential, and a court would likely find both subjective and objective expectations of privacy. It remains to be seen whether the Supreme Court agrees.

B. THE FOURTH AMENDMENT AND THIRD PARTIES

As an initial matter, the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy.[69] Nor does the *right* of access.[70]

In *Katz v. United States*, telephone companies had both the ability and right to monitor calls, yet the Supreme Court found a reasonable expectation of privacy during a telephone call.[71] Likewise, letters and other sealed packages carry with them an expectation of privacy for the sender,[72] despite the fact that they are handed over to numerous mail carriers and are subjected to the risk that any mail handler "could tear open the thin paper

67. *Privacy in the Digital Age: Encryption and Mandatory Access: Hearing Before the Subcomm. on the Constitution, Federalism, & Prop. Rights of the Comm. on the Judiciary*, 105th Cong. 4 (1998) (statement of Sen. Russell D. Feingold), *available at* http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

68. *Id.*; *but see* United States v. Taketa, 923 F.2d 665, 673 (9th Cir. 1991) (noting that if a court allowed the existence of a master key to overcome the expectation of privacy, it would defeat the legitimate privacy interest of any hotel, office, or apartment occupant, which our courts are not prepared to do). Thus, the existence of a master key may not impact a court's analysis of a "reasonable expectation of privacy."

69. *Warshak*, 631 F.3d at 286; *see also* Katz v. United States, 389 U.S. 347, 353 (1967) (concluding that the government's access to a telephone conversation did not destroy the reasonable expectation of privacy).

70. *Warshak*, 631 F.3d at 287.

71. *Katz*, 389 U.S. at 353, 359; *see also* Smith v. Maryland, 442 U.S. 735, 746–47 (1979) (Stewart, J., dissenting) (stating that the telephone conversation in *Katz* "must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment").

72. United States v. Jacobsen, 446 U.S. 109, 114 (1984).

envelopes that separate the private words from the world outside."[73] Even the degree of access that Internet Service Providers ("ISPs") have over email accounts does not necessarily diminish a reasonable expectation of privacy in an individual's email.[74]

Conversely, there are times when individuals assume the risk that the third party to whom they convey information may subsequently reveal that information to the government. This most often occurs when the information is "voluntarily" turned over or "knowingly exposed" to a third party.[75]

1. The Third-Party Doctrine & Voluntary Revelation

Under Supreme Court precedent, information that is voluntarily revealed to third parties does not warrant Fourth Amendment protection.[76] Instead, this voluntary act of disclosure invokes the third-party doctrine, which gives the government additional leeway in obtaining "so-called private" information. Essentially, the third-party doctrine "postulates that if the information in question has been voluntarily turned over to a third party, the individual seeking privacy protection no longer has a reasonable expectation of privacy."[77]

Smith v. Maryland is a notable case for this doctrine. Here the Court found that individuals lack a reasonable expectation of privacy in the numbers they dial on a telephone.[78] To use a phone, an individual must type in numbers to connect with another party, and such an act "voluntarily convey[s] numerical

73. *Warshak*, 631 F.3d at 285.

74. *Id.* at 287 (noting that the ISP subscriber agreement specifically stated that the ISP "*may* access and use individual Subscriber information," but that the degree of access did not diminish the reasonable expectation of privacy in emails).

75. *See, e.g.*, *Katz*, 389 U.S. at 351 (finding that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection"); Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043 (D.C. Cir. 1978) ("To the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protection").

76. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004) ("The Supreme Court has repeatedly held, however, that the Fourth Amendment does not protect information revealed to third parties."); *see also Smith*, 442 U.S. at 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976); United States v. White, 401 U.S. 745, 749, 754 (1971).

77. Lindsay M. Gladysz, Note, *Status Update: When Social Media Enters the Courtroom*, 7 I/S: J. L. & POL'Y FOR INFO. SOC'Y 688, 708 (2012); *see also* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

78. *Smith*, 442 U.S. at 744–46. *But cf. In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (noting that although cellphone customers may voluntarily share phone numbers dialed, they do not voluntarily share cell site location information).

information to the telephone company"[79] as individuals must know that phone companies have "facilities for making permanent records of the numbers they dial . . . ."[80] As a result, a "person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[81] However, it is unlikely that cellphone customers are aware that their cellphone providers collect any additional information aside from numbers dialed into the phone.[82] Thus, whether the expectation of privacy is "one that society is prepared to recognize as reasonable" is dependent, at least in part, on whether information is *voluntarily* conveyed and *knowingly* used.[83]

2. Third Parties and the Content versus Non-Content Context

In analyzing cases involving third parties, another way to characterize the split is through the content versus non-content divide.[84] The distinction between *Smith* and *Katz* most prominently lies in the difference between non-content information (often thought of as metadata)[85] and content information.

In *Smith* and its subsequent line of cases, courts have upheld the notion that users do not have a "reasonable expectation of privacy in their subscriber information, the length of their stored files, and other *non-content* data to which service providers must have access"[86] (such as phone numbers

79. *Smith*, 442 U.S. at 744.

80. *Id.* at 742.

81. *Id.* at 743–44; *see also Miller*, 425 U.S. at 442 (holding that a bank depositor does not a have a legitimate expectation of privacy in the "financial statements and deposits slips . . . voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business").

82. Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Affirmance, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866619 (arguing that "when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed"). *But see In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013) (finding that "users know that they convey information about their location to their service providers when they make a call and that they voluntarily continue to make such calls").

83. *Smith*, 442 U.S. at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

84. *See, e.g.*, 18 U.S.C. § 2703(a)–(c) (2012) (differentiating the standards for required disclosure of customer communications, 18 U.S.C. § 2703(a)–(b), versus records, 18 U.S.C. § 2703(c)); *Smith*, 442 U.S. at 741 (noting that pen registers differ significantly because they "do not acquire the *contents* of communications") (emphasis added).

85. *A Guardian Guide to Your Metadata*, THE GUARDIAN (June 12, 2013, 11:52 AM), http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1100000.

86. United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. 2007), *vacated*, 648 F.3d 1 (1st Cir. 2011); *see also Smith*, 442 U.S. at 741 (noting that pen registers differ significantly because they "do not acquire the *contents* of communication"); *In re* U.S. for

dialed and a sender's name, email address, and IP address). Thus, service providers can be forced to disclose this information to the government without implicating the Fourth Amendment. Conversely, the *contents* of communications, such as the actual message and items that are not directed to the third-party intermediary (such as the ISP), but rather to a specific recipient, are generally protected under the Fourth Amendment.[87] In *Katz* and its line of cases, where the service provider is merely the intermediary, the content-based communications between parties continue to give the user a reasonable expectation of privacy, and therefore the Fourth Amendment protects messages.[88]

Taking into account the different roles of third parties in the content versus non-content scenarios, the Fourth Amendment analysis may just hinge on the position of the third party in relation to the information; specifically, "whether the third party created the record to memorialize its business transaction with the target" (non-content records), or rather the third party "simply record[ed] its observation of a transaction between two independent parties" (content data).[89] Where the third party simply records its observation of the transaction (such as recording email exchanges between parties), and is not a party to the transaction, the content is subject to Fourth Amendment protection.[90] However, where the third party collects and stores non-content information (such as recording customer subscription information like email to/from addresses or the telephone numbers dialed) for its own business purposes or for routing the communication, the third party becomes a party to the transaction and the Fourth Amendment does not protect such information. Thus, "[c]ommunications content, such as the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business, are generally protected. However, addressing information, which the business needs to route those communications appropriately and efficiently are not."[91]

Historical Cell Site Data, 724 F.3d at 611–12 (holding that cell site information is a business record to which the cell service provider is a party and as such falls into the non-content bucket); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (holding that a user loses any expectation of privacy in personal subscription information when it is conveyed to a system operator).

87. *See In re* U.S. for Historical Cell Site Data, 724 F.3d at 611 ("Communications content, such as the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business, are generally protected. However, addressing information, which the business needs to route those communications appropriately and efficiently are not.").

88. *See, e.g.*, *Katz*, 389 U.S. at 352 (1967); Warshak, 631 F.3d at 286, 288.

89. *In re* U.S. for Historical Cell Site Data, 724 F.3d at 611.

90. *See, e.g.*, *Warshak*, 631 F.3d at 286, 288.

91. *In re* U.S. for Historical Cell Site Data, 724 F.3d at 611.

3. The Employer Context

Expectations of privacy become more complicated when the third-party intermediary is an employer. Even more uncertainty abounds if the employer has a policy of monitoring electronic communications. This is because the reasonableness of a privacy expectation in the employment setting "is understood to differ according to context."[92] Nevertheless, individuals do not lose all Fourth Amendment rights in the employment setting.

"In both the public and private sectors, employees' privacy rights are governed by whether or not the employee had a reasonable expectation of privacy."[93] Although private sector employers are bound by the common law right to privacy—most often, a tort for the invasion of privacy—and as such fall outside of the scope of this Article, in the public sector, employer privacy rights are defined by constitutional principles under the Fourth Amendment.[94] This distinction is important because there are "more than 23 million government (federal, state, and local) employees in the United States, and, at least as a default matter, they have some claim to privacy while at work."[95]

O'Connor v. Ortega[96] sets forth the analytical framework for Fourth Amendment claims against public sector employers. There, the Supreme Court noted the importance of balancing the legitimate privacy interests of public employees with the realities of the workplace.[97] Ultimately, the Court

92. O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

93. Molly DiBianca, *Is There a Reasonable Expectation of Privacy in Your Tweets?*, DEL. EMP. L. BLOG (July 23, 2013), http://www.delawareemploymentlawblog.com/2013/07/is-there-a-reasonable-expectation-of-privacy-in-your-tweets.html; *see also* TIMOTHY P. GLYNN, RACHEL ARNOW-RICHMAN, AND CHARLES A. SULLIVAN, EMPLOYMENT LAW: PRIVATE ORDERING AND ITS LIMITATIONS 349–50 (2d ed. 2011) ("In order for an employee or applicant to have a cognizable breach of privacy claim (of any kind), he or she must have a legitimate or reasonable expectation of privacy in the sphere upon which the employer intruded."). However, "the sources of privacy protection analyzed in each case [(i.e., public employer versus private employer)] are different." *Id.* Many courts faced with private sector privacy cases have borrowed from government employer cases, asking whether the employee had a reasonable expectation of privacy. *See, e.g.*, O'Bryan v. KTIV Television, 868 F. Supp. 1146, 1159 (N.D. Iowa 1994); K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 638 (Tex. App. 1984).

94. *See, e.g.*, *O'Connor*, 480 U.S. at 717 ("Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer."); Nat'l Treasury Emp. Union v. Von Raab, 489 U.S. 656, 665 (1989) ("Our earlier cases have settled that the Fourth Amendment protects individuals from unreasonable searches conducted by the Government, even when the Government acts as an employer."); DiBianca, *supra* note 93.

95. TIMOTHY P. GLYNN, RACHEL ARNOW-RICHMAN, AND CHARLES A. SULLIVAN, EMPLOYMENT LAW: PRIVATE ORDERING AND ITS LIMITATIONS 301 (2d ed. 2011).

96. 480 U.S. 709 (1987).

97. *Id.* at 721.

found that a physician at a state hospital did not lose his Fourth Amendment rights solely because of his decision to work for the government.[98] Instead, the physician enjoyed an expectation of privacy in his desk and file cabinets, as he did not share these items with other employees.[99] The Court, however, disagreed on precisely how to apply the reasonable expectation of privacy analysis in the public sector employment context, and the test remains unclear to this day.[100] In fact, in the most recent Supreme Court case on this issue, the Court proceeded with care in determining privacy expectations for employer-owned electronic equipment.[101]

More often than not, employer policies, or lack thereof, will shape the reasonableness of a privacy expectation.[102] In many cases where public employers do not have formal policies allowing inspections of employee activities, courts have found both a subjective and objective reasonable expectation of privacy,[103] though not always a violation of the Fourth Amendment.[104] However, as a condition of employment and through the use of employer-provided technology, many employees effectively waive their

98. *Id.* at 718–19.

99. *Id.*

100. *See id.*; *see, e.g.*, City of Ontario v. Quon, 560 U.S. 746, 759 (2010) (finding that it was preferable to dispose of the case on narrower grounds because, "[e]ven if the Court were certain that the *O'Connor* plurality's approach were the right one, the Court would have difficulty predicting how employees' privacy expectations will be shaped" by rapidly changing technology).

101. *Id.* at 759 ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

102. *See, e.g.*, *id.* at 760 (finding that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated").

103. *See, e.g.*, Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1335 (9th Cir. 1987) (finding that an employee "would enjoy a reasonable expectation of privacy in areas given over to his exclusive use, unless he was on notice from his employer that searches of the type to which he was subjected might occur from time to time for work-related purposes"), *abrogated by* Pollard v. The GEO Grp., Inc., 629 F.3d 843 (9th Cir. 2012), *rev'd sub nom.* Minneci v. Pollard, 132 S. Ct. 617 (2012); Gillard v. Schmidt, 579 F.2d 825, 828 (3d Cir. 1978) (holding that "in the absence of an accepted practice or regulation to the contrary," a school employee "[w]orking in an office secured by a locked door" had a reasonable expectation of privacy in his desk and its contents).

104. This is largely due to the plurality's opinion in *O'Connor* stating that internal investigations into work-related misconduct should instead be judged by a standard of reasonableness. *See O'Connor*, 480 U.S. at 725–26; United States v. Taketa, 923 F.2d 665, 673–74 (9th Cir. 1991) (finding the search of an employee's office subject to Fourth Amendment restraints but where the search was directed at uncovering work-related misconduct, the warrantless search was in-line with the *O'Connor* Court's analysis and not in violation of the Fourth Amendment).

expectation of privacy and are effectively on notice of employer intrusion into their private space (both physical and electronic).[105]

In cases where public employers have formal policies that sufficiently provide notice to employees that their communications and files may be monitored, employees lose their objectively reasonable expectation of privacy.[106] *United States v. Simmons* is a perfect example.[107] There, the government employer had an internet policy that clearly stated that the employer would "audit, inspect, and/or monitor an employee's use of the internet."[108] As a result, the court concluded that such "office practices, procedures, or regulations may reduce legitimate privacy expectations."[109] Regardless of whether the employee had a "subjective" expectation of privacy in his internet usage, the internet policy effectively negated an "objective" expectation of privacy.[110] Subsequently, when the government employer conducted remote searches of the employee's computer, the employee's Fourth Amendment rights were not violated, since the employee lacked "a legitimate expectation of privacy in the files downloaded from the internet."[111]

4. What about Passwords?

The status of passwords within the morass of the third-party doctrine remains unknown. Under the content versus non-content distinction noted above in Subsection III.B.2, one might argue that passwords should be

105. *See, e.g.*, *O'Connor*, 480 U.S. at 717 ("Public employees' expectations of privacy . . . may be reduced by virtue of actual office practices and procedures."); Pauline T. Kim, *Electronic Privacy and Employee Speech*, 87 CHI.-KENT L. REV. 901, 919 (2012); Lewis Maltby, *Employment Privacy: Is There Anything Left*, HUM. RTS., 2013, *available at* http://www.americanbar.org/publications/human_rights_magazine_home/2013_vol_39/may_2013_n2_privacy/employment_privacy.html ("The actual test of whether an employee has a reasonable expectation of privacy is who owns the equipment used to transmit the message. If the equipment belongs to the employer, the employer has the right to monitor anything and everything on it.").

106. *See, e.g.*, Biby v. Bd. of Regents of Univ. of Neb. at Lincoln, 419 F.3d 845, 850–51 (8th Cir. 2005) (finding an employee does not have a reasonable expectation of privacy in his computer files where the employer's computer policy allows for searches); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002) (finding that the employer's "policies and procedures prevent its employees from reasonably expecting privacy in data downloaded from the Internet onto University computers"); United States v. Hamilton, 778 F. Supp. 2d 651, 654 (E.D. Va. 2011) (finding that a public school employee lacked an objectively reasonable expectation of privacy in emails stored on his work computer since he had been on notice that contents of his computer were subject to inspection).

107. 206 F.3d 392, 398–99 (4th Cir. 2000).

108. *Id.* at 398.

109. *Id.*

110. *Id.*

111. *Id.*

considered non-content information and therefore their compelled disclosure would not violate an individual's Fourth Amendment rights. This is a plausible argument; a password for an electronic device resembles telephone digits entered into a phone, as passwords often have to be entered in order to actually utilize the device. And, passwords are, after all, the key to unlocking the content, and a third party can theoretically record them. However, when viewed in totality, passwords should be treated like the *contents* of communication. Although passwords in the traditional sense may have functioned simply as a key to unlocking data, such an analogy fails in the digital age. At least in the form of decryption keys, passwords change content from unreadable to readable text, thereby communicating information.[112] Despite the uncertainty of whether passwords are content or non-content data, the role of third parties in relation to passwords is not "sufficient to extinguish a reasonable expectation of privacy,"[113] and thus should help to correctly place passwords in the *Katz* line of cases.

First, numerous third-party service providers do not record password information. Instead, third-party service providers often have only the ability to reset the password should a user forget it.[114] Second, although third-party employers and some service providers may actually have access to this information,[115] individuals do not assume that passwords are used by their

112. *See In re* Under Seal, 749 F.3d 276, 279 (4th Cir. 2014) (noting that decryption is the process of changing ciphertext (an unreadable jumble of letters and numbers) back into plaintext (readable data)); *see also* Brief for the ACLU Found. of Mass et al. as Amici Curiae Supporting Defendant at 5–7, 19–20, Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014) (No. SJC-11358), *available at* https://www.eff.org/files/2013/10/29/brief_of_amici_curiae_aclum_aclu_eff.pdf.

113. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

114. *See, e.g.*, JOSEPH BONNEAU & SÖREN PREIBUSCH, THE PASSWORD THICKET: TECHNICAL AND MARKET FAILURES IN HUMAN AUTHENTICATION ON THE WEB 19 (2010), *available at* http://weis2010.econinfosec.org/papers/session3/weis2010_bonneau.pdf ("The best solution, sending a time-limited reset link . . . was implemented about half of the time, with identity sites being very significantly more likely to implement this."); *Apple ID: Changing Your Password*, APPLE SUPPORT, http://support.apple.com/en-us/HT201355 (last modified Dec. 11, 2014) (detailing steps to changing your Apple ID password) [hereinafter *Apple ID*]; *Customer Proprietary Network Information (CPNI) for Wireless Consumers*, VERIZON, http://www.verizonwireless.com/b2c/globalText?contentType=Legal%20Notice&textId=181 (last visited Jan. 3, 2015) (noting that the information collected includes "services purchased (including specific calls you make and receive), related local and toll billing information, the type, destination, technical configuration, location and amount of use of purchased services," but does not mention passwords) [hereinafter *CPNI*]. *But see AT&T Privacy Policy*, AT&T, http://www.att.com/gen/privacy-policy?pid=2506 (last updated Sept. 16, 2013) (noting that AT&T collects account information such as security codes).

115. With regard to the employment context, see *Keylogging Employees' Computer Use Met with Judicial Wariness*, JACKSON LEWIS (June 5, 2009), http://www.jacksonlewis.com/legalupdates/article.cfm?aid=1747 (discussing a case in which an employer used keylogging to discover an employee's password) [hereinafter JACKSON LEWIS].

providers for any legitimate business purpose, nor do users of electronic devices necessarily know that third parties have facilities for making permanent records of the passwords they enter.[116] Additionally, users of electronic devices do not voluntarily hand over their password when entering it into their device.[117] Instead, users assume that only they know the password,[118] since "[t]he important feature about PINs and passwords is that they're generally something that we know"[119] and that have to be recalled through personal memory and usually cannot be directly regained through a "forgot my password" option. Finally, although less clear, third parties may be viewed as mere intermediaries because third parties do not create password records to memorialize the business transaction with the individual; the user creates his own password independent of the business transaction with his service provider.[120]

Moreover, because most service providers do not even collect or store passwords,[121] the third-party doctrine should not be considered in assessing a user's reasonable expectation of privacy in his passwords. Even if some service providers collect passwords, customers generally are not aware that phone companies are recording this information,[122] thereby negating the

116. Brief of Amici Curiae Electronic Frontier Foundation et al., *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 386619 (arguing that "when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed"). However, it is worth noting that "[t]o the extent an individual *knowingly* exposes his activities to third parties, he surrenders Fourth Amendment protections." Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043 (D.C. Cir. 1978) (emphasis added).

117. *See supra* Section III.B.

118. *See, e.g.*, *CPNI*, *supra* note 114; *Apple ID*, *supra* note 114. *But see AT&T Privacy Policy*, *supra* note 114.

119. Marcia Hoffmann, *Apple's Fingerprint ID May Mean You Can't "Take the Fifth*," WIRED (Sept. 12, 2013), http://www.wired.com/opinion/2013/09/the-unexpected-result-of-fingerprint-authentication-that-you-cant-take-the-fifth/.

120. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013) (noting that "the right to possession hinges on whether the third party created the record to memorialize its business transaction with the target"). For a discussion of the implications of third parties who serve as intermediaries, see *supra* Subsection III.B.2.

121. Angwin, *supra* note 2, at B4 ("Spokeswomen for Microsoft Corp. and Research In Motion Ltd. say their companies don't collect or store passwords."). Even if service providers "store" passwords, in technical terms, they are "hashed and salted"—a one-way cryptographic strategy that allows an application to authenticate a user without the ability to read their password. *Salted Password Hashing—Doing it Right*, CRACKSTATION, https://crackstation.net/hashing-security.htm (last modified Aug. 6, 2014, 7:12 PM).

122. Brief of Amici Curiae Electronic Frontier Foundation et al., *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 386619 (arguing that "when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed

third-party doctrine. Courts should therefore treat passwords like email given the similar nature of the sensitive information conveyed in both, and should determine that the "the degree of access granted to [third parties] does not diminish the reasonableness"[123] of privacy in passwords.

Despite the argument that passwords should be protected under the Fourth Amendment, there might be a caveat in the employment context. Because an employee's expectation of privacy in an employment setting depends heavily on an employer's policies, practices, procedures and regulations,[124] whether employees have an expectation of privacy in their passwords on employer-owned electronic devices is subject to a case-by-case analysis. When an employer has a policy notifying employees that both their electronic communications will be monitored and that keystroke logging will be used to track and record *anything* typed into a device, courts should assume that such employees do not have an "objectively" reasonable expectation of privacy. In these limited circumstances, courts should employ an employment caveat for privacy protections and not afford Fourth Amendment protection to passwords. But in a situation where an employer's policies and procedures give employees notice that their computer-activity is being monitored but do not mention the use of keystroke logging (an important practice in being able to record passwords typed into a device), a grey area would remain. In this grey area, an employee should still have a reasonable expectation of privacy, both subjective and objective, in passwords typed into employer-provided devices, until keystroke logging is common practice and the subject of widespread awareness in all workplace settings,[125] thereby negating an "objectively" reasonable expectation.

---

to the phone company is the number that is dialed"). *But see In re* U.S. for Historical Cell Site Data, 724 F.3d at 612 (finding that "users know that they convey information about their location to their service providers when they make a call and that they voluntarily continue to make such calls").

123. *See* United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010).

124. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 717 (1987) ("Public employees' expectations of privacy . . . may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."); United States v. Angevine, 281 F.3d 1130, 1134–35 (10th Cir. 2002) (citing *O'Connor v. Ortega* and noting that "Oklahoma State University policies and procedures prevent its employees from reasonably expecting privacy in data downloaded from the Internet onto University computers"); People v. Kent, 910 N.Y.S.2d 78, 92–93 (2010) ("An employee's expectation of privacy in material stored in an office computer depends upon the employer's policy regarding computer use and any other relevant office practices, procedures, and regulations.").

125. As it is, keystroke logging "is done secretly, so the person using the keyboard is unaware his activities are being monitored." JACKSON LEWIS, *supra* note 115.

IV. ATTEMPTS AT PROTECTING PASSWORDS UNDER THE FIFTH AMENDMENT

Although the Fourth Amendment protects individuals by keeping secure their persons, papers, and effects against unreasonable seizures, it still allows the government to obtain Fourth Amendment–protected information through a narrowly-tailored search warrant based on probable cause.[126] But if the information compelled by the search warrant is testimonial and incriminating, then the legal analysis shifts to the Fifth Amendment.

A. ESTABLISHING THE REQUIREMENTS TO INVOKE THE FIFTH AMENDMENT

Under the Fifth Amendment, "[n]o person shall be . . . compelled in any criminal case to be a witness against himself."[127] In order to invoke this right, an individual must establish three things: (1) compulsion, (2) a testimonial communication, and (3) incrimination.[128]

(1) Compulsion. Under the Fifth Amendment, compulsion requires that the government force an individual to surrender information.[129] Essentially, courts must decide if testimony is free and voluntary or if it was obtained through improper influence.[130] If the latter is found to be true, courts view this "extortion of information from the accused himself [as] offen[sive] [to] our sense of justice."[131]

(2) Testimonial. In order for the act to be "testimonial" under the Fifth Amendment, the result of revealing the information must cause a person to be a "witness" against himself.[132] Essentially, the communication must force the individual into "the cruel trilemma," compelling the individual to choose between self-accusation, perjury or contempt when asked to give a sworn

126. Kerr, *supra* note 76, at 1211–14.

127. U.S. CONST. amend. V.

128. Shields, *supra* note 11.

129. *See, e.g.*, Fisher v. United States, 425 U.S. 391, 397 (1976) (finding the Fifth Amendment serves to prohibit the use of "physical or moral compulsion" on a person asserting privilege); Boyd v. United States, 116 U.S. 616, 630 (1886) (holding that "any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime" violated the Fourth and Fifth Amendments).

130. *See* Bram v. United States, 168 U.S. 532, 542–43 (1897) (holding that the constitutional inquiry is whether the confession was "free and voluntary: that is, must not be extracted by any sort of threats or violence, nor obtained by any direct or implied promises, however slight, nor by the exertion of any improper influence") (internal citations omitted).

131. Couch v. United States, 409 U.S. 322, 328 (1973).

132. *See* Doe v. United States, 487 U.S. 201, 210 (1988) ("[I]n order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself.").

statement containing factual information.[133] This privilege does not extend to the production of real or physical evidence,[134] but does protect expressions of content in an individual's mind.[135] And an act is not testimonial if the information revealed is already known by the government—a "foregone conclusion."[136]

(3) Incrimination. Additionally, the compelled testimonial communication must be incriminating. Courts must determine whether the revelation of the testimony would create a substantial hazard of self-incrimination or otherwise expose an individual to a criminal charge.[137]

However, an important limitation of the Fifth Amendment must be noted: the protection of the Fifth Amendment is limited to when an individual is "compelled to be a witness against himself."[138] The Supreme Court has repeatedly held that the Fifth Amendment was never intended to allow a person to argue that some other person "might be incriminated by his testimony."[139] This is true even if that person can be classified as an agent of the other person.[140] Thus, the incrimination provision may allow individuals to claim Fifth Amendment protection, but it leaves no redress for third parties compelled to hand over passwords to the government.

B. COMPELLING PASSWORDS FROM INDIVIDUALS: DOESN'T THAT VIOLATE THE FIFTH AMENDMENT?

Lately, the government has become aggressive in its quest for passwords.[141] And while individuals have been quick to fight back with the Fifth Amendment privilege, courts have diverged in deciding whether the privilege does in fact protect passwords.

In 2012 the Eleventh Circuit ruled on the issue of whether a defendant could be required to decrypt an encrypted hard drive without implicating the Fifth Amendment.[142] In that case, the defendant was served with a subpoena

133. *See* Pennsylvania v. Muniz, 496 U.S. 582, 596 (1990).

134. *See id.* at 589 ("[W]e have long held that the privilege does not protect a suspect from being compelled by the State to produce 'real or physical evidence.' ").

135. *See Doe*, 487 U.S. at 210 n.9.

136. United States v. Hubbell, 530 U.S. 27, 44 (2000).

137. *See* United States v. Reis, 765 F.2d 1094, 1095 (11th Cir. 1985) (the witness "must be faced with substantial and real hazards of self-incrimination"); Hale v. Henkel, 201 U.S. 43, 67 (1906).

138. Fisher v. United States, 425 U.S. 391, 398 (1976).

139. *Hale*, 201 U.S. at 69; *see also Fisher*, 425 U.S. at 398.

140. *See Fisher*, 425 U.S. at 397.

141. *See, e.g.*, Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614 (Mass. 2014); Angwin, *supra* note 2, at B4; Farivar, *supra* note 2.

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

because forensic examiners were unable to view the encrypted portions of his seized laptops and external hard drives.[143] The subpoena required him to produce the unencrypted *contents* located on the hard drives of his laptops and five external hard drives.[144] He refused to comply, invoking his Fifth Amendment privilege against self-incrimination.[145] Although the government conceded that the decryption and production of the data would be "compelled" and "incriminatory," the government disputed whether it would also be "testimonial."[146] The Eleventh Circuit, reversing the district court, found that the defendant's "decryption and production of the hard drives' contents would trigger Fifth Amendment protection because it would be testimonial."[147] Despite the government's argument that it was not seeking "the combination or key, but rather the contents," the court found that production would still require the individual to use "the contents of his own mind" to decrypt the files.[148] The court centered its analysis on the act of production, finding the Fifth Amendment protected against production and decryption of the hard drives.[149]

Notwithstanding the Eleventh Circuit's guidance, a state supreme court has recently ruled that individuals can be compelled to divulge passwords when the information that would be disclosed is a "foregone conclusion."[150] In *Commonwealth v. Gelfgatt*, the Massachusetts Supreme Court conceded that entering an encryption key would appear to be a "testimonial communication. . .trigger[ing] Fifth Amendment protection," but noted that it also had to determine whether the act of production would "lose[] its testimonial character" because the information would be a "foregone conclusion."[151] And because the defendant's "ownership and control of the computers," "knowledge of the fact of encryption," and "knowledge of the encryption key" were already known, the court concluded that entering an encryption key in this case was a "foregone conclusion" and therefore was not a testimonial communication protected by the Fifth Amendment.[152]

143. *Id.* at 1340.
144. *Id.*
145. *Id.* at 1337.
146. *Id.* at 1341–42.
147. *Id.* at 1341.
148. *Id.* at 1345–46. The Supreme Court has long held that forcing the accused "to disclose the contents of his own mind" implicates the Fifth Amendment. *See, e.g.*, Curcio v. United States, 354 U.S. 118, 128 (1957).
149. *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d at 1346.
150. Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614 (Mass. 2014).
151. *Id.*
152. *Id.* at 615.

This split in opinion has played out in the district courts over the last several years. While some courts have agreed with the Eleventh Circuit, finding that compelling an individual's password would infringe on his Fifth Amendment self-incrimination privilege,[153] others have found exceptions to an individual's claim of Fifth Amendment privilege. In the former category lies *United States v. Kirschner*, where the government subpoenaed a defendant to divulge the password to his computer,[154] but the court found that providing the password would be like giving the combination to a safe and would be a testimonial communication.[155] In contrast, other courts have bypassed the Fifth Amendment privilege by: (1) compelling defendants to provide an unencrypted version of the hard drive, but not the passwords, where the subpoena requested passwords to the computer;[156] (2) being amenable to government requests for the *contents* of the encrypted data;[157] and (3) finding that decryption is not testimonial when the information sought to be obtained is already known.[158] In these cases, only the underlying data, not the passwords, were revealed. [159] However, as the approaches taken by the lower courts further diverge, the issue may soon make its way up to the Supreme Court.

153. United States v. Kirschner, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010); *see also* United States v. Rogozin, No. 09-CR-379(S)(M), 2010 WL 4628520, at *6 (W.D.N.Y. Nov. 16, 2010) (holding that the defendant's statement as to his password was testimonial in nature and recommending suppression of the statement).

154. *Kirschner*, 823 F. Supp. 2d at 668.

155. *Id.*

156. *See, e.g.*, *In re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *1, *4 (D. Vt. Feb. 19, 2009) (directing the defendant to provide an unencrypted version of hard drive where the government's expert was unable to search a computer because of password-protection and where the subpoena had asked for "any passwords associated with the laptop"). It is worth noting that in *In re* Boucher (*Boucher I),* No. 2:06–mj–91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007), the magistrate judge found the act of producing the password was testimonial and privileged, and as a result, on appeal, the request for a password was revised to a request for an unencrypted version of the hard drive. *Boucher II*, 2009 WL 424718, at *2.

157. *See* United States v. Fricosu, 841 F. Supp. 2d 1232, 1235, 1238 (D. Colo. 2012) (holding that defendant shall provide an unencrypted copy of her computer's hard drive to the government where the government sought a writ for the unencrypted contents).

158. *See, e.g.*, *In re* Decryption of a Seized Data Storage System, No. 13-M-449, at 3 (E.D. Wis. filed May 21, 2013) (order granting ex parte request for reconsideration), *available at* http://www.wired.com/images_blogs/threatlevel/2013/05/decryptorder.pdf.

159. But, at least one court has forced an individual to hand over their passwords to social networking sites. *See* McMillen v. Hummingbird Speedway Inc., No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *13 (Pa. Ct. Com. Pl. Sept. 9, 2010) (ordering plaintiff to "provide his Facebook and MySpace user names and passwords to counsel").

Finally, it is important to recognize that a password or an encryption key alone would not by itself be incriminating—only testimonial.[160] However, when the information behind the "lock" is incriminating, providing the combination would trigger the privilege.[161] And while password "locks" could be written down, they usually lie solely in one's mind—thus causing an individual to use "the contents of his own mind" to divulge this information, and thereby triggering Fifth Amendment testimonial protections.[162] However, if the government were to require manufacturers or users of encryption keys to keep a copy of the keys,[163] the testimonial compulsion would likely disappear along with the Fifth Amendment privilege, as the password would no longer lie solely in one's mind. Likewise, if password authentication systems move from combinations to biometrics, such as fingerprints (a likely possibility given Apple's use of fingerprints to unlock some iPhones), the government could demand biometric passwords without implicating the Fifth Amendment[164] because the Supreme Court has decided that biometrics are not testimonial.[165]

160. *See, e.g.*, Fisher v. United States, 425 U.S. 391, 410 (1976) (concluding that an act of production is testimonial if it concedes the existence, possession, control and authenticity of the documents); *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1345 (11th Cir. 2012) (holding that "an act of production can be testimonial when that act conveys some explicit or implicit statement of fact that certain materials exist, are in the subpoenaed individual's possession or control, or are authentic"); Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CONST. L. HEIGHT. SCRUTINY 11, 24 (2012) ("Courts generally agree that divulging a password constitutes a testimonial act.").

161. Engel, *supra* note 11, at 556.

162. Hoffmann, *supra* note 119, at 2 ("These memory-based authenticators are the type of fact that benefit from strong Fifth Amendment protection should the government try to make us turn them over against our will.").

163. *Privacy in the Digital Age: Encryption and Mandatory Access: Hearing Before the Subcomm. on the Constitution, Federalism, & Prop. Rights of the Comm. on the Judiciary*, 105th Cong. 14 (1998) (testimony of Robert S. Litt, Principal Assoc. Deputy Att'y Gen.), *available at* http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

164. *See, e.g.*, Virginia v. Baust, No. CR14-1439, 2014 WL 6709960, at *3 (Va. Cir. Ct. Oct. 28, 2014) (holding that a "[d]efendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same," because his "fingerprint, like a key, . . . does not require the witness to divulge anything through his mental processes"); Hoffmann, *supra* note 119, at 2 ("[I]f we move toward authentication systems based solely on physical tokens or biometrics—things we have or things we are, rather than things we remember—the government could demand that we produce them without implicating anything we know."); Jack Linshi, *Why the Constitution Can Protect Passwords But Not Fingerprint Scans*, TIME (Nov. 6, 2014), http://time.com/3558936/fingerprint-password-fifth-amendment/.

165. *See* Gilbert v. California, 388 U.S. 263, 266–67 (1967) (finding that a suspect may be compelled to provide a handwriting exemplar); Schmerber v. California, 384 U.S. 757, 765 (1966) (finding that a suspect may be compelled to furnish a blood sample).

C. ADDITIONAL CIRCUMVENTIONS OF THE FIFTH AMENDMENT

Even if the Supreme Court were to hear a case to resolve the divergent approaches of the courts and find a Fifth Amendment privilege for individuals, the question remains: what is left of an individual's Fifth Amendment password protection when it can be circumvented by getting the information from a third party? All of the cases above involve instances where the government compelled passwords from the creator of the password. They do not address how a court would analyze a situation in which a password is stored on the servers of an innocent third party. Because the Fifth Amendment is "not implicated when the government tries to compel passwords from third parties,"[166] the fact that the data is located on a third party's servers may destroy the individual's Fifth Amendment protections. The text of the Fifth Amendment specifically limits this privilege to one compelled to be a "witness against himself."[167] And the Supreme Court has found that the Fifth Amendment does not play any role when a third party is resisting disclosure of information to protect somebody else.[168] In essence, the Fifth Amendment provides a weak protection for individuals in protecting their digital footprint. The government's ability to compel passwords from third parties undermines the legal rights individuals currently enjoy under the Fifth Amendment and essentially renders the Fifth Amendment useless in protecting an individual's digital incriminating communications.

Although technology has changed, privacy rights should not. But as the law currently stands, passwords can be obtained by carefully navigating around two constitutional amendments that implicate privacy concerns. Even if passwords are protected under the Fourth Amendment, they can still be obtained through a narrowly-tailored search warrant based on probable cause. And, while an individual may then be able to invoke the Fifth Amendment to protect their passwords from disclosure, a third party could not. Thus, passwords could be easily obtained by serving a search warrant on a third party, complying with the Fourth Amendment without implicating the Fifth Amendment—a troublesome notion that the drafters of the Fifth Amendment surely did not anticipate. If the Fifth Amendment will not bar

166. Orin Kerr, *US Government Getting Password Information? (And Why the Story Raises More Questions than Answers)*, VOLOKH CONSPIRACY (July 26, 2013, 2:43 PM), http://www.volokh.com/2013/07/26/u-s-government-getting-password-information-and-why-the-story-raises-more-questions-than-answers/.

167. U.S. CONST. amend. V.

168. *See, e.g.*, Fisher v. United States, 425 U.S. 391, 398 (1976); Hale v. Henkel, 201 U.S. 43, 69 (1906).

the government from the compulsory extortion of an individual's private passwords from a third party, then other laws should step in.

V. INADEQUACY OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

As technology has evolved, the Electronic Communications Privacy Act (ECPA)[169] has not. Enacted in 1986[170]—when the commercial internet did not exist and cellphones were too heavy and expensive to be easily used—the ECPA purports to protect the privacy of Americans' electronic lives.[171] Congress enacted the ECPA "to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunication technologies,"[172] intending to "fairly balance . . . the interests of privacy and law enforcement."[173] Congress enacted the Stored Communications Act ("SCA") as Title II of the ECPA to address voluntary and compelled disclosure of "stored wire and electronic communication and transactional records" held by third-party service providers because the internet created a host of privacy issues for users that may not have been adequately protected by the Fourth Amendment.[174] The SCA "creates rights [for] 'customers' and 'subscribers' of . . . service providers in both content and non-content information held by two particular types of providers:"[175] electronic communication service ("ECS") [176] providers (such as telephone

169. 18 U.S.C. §§ 2510–2522 (2012).

170. The ECPA was enacted just two years after Super Mario burst into homes on Nintendo (1984), *Nintendo History*, NINTENDO, https://www.nintendo.co.uk/Corporate/Nintendo-History/Nintendo-History-625945.html (last visited Jan. 6, 2015); three years before Zack Morris was spotted carrying a five-pound cellphone on Saved by The Bell (1989), ZACK MORRIS CELL PHONE.COM, http://zackmorriscellphone.com/ (last visited Jan. 2, 2015); and more than twenty years before Apple released the first iPhone (2007), *7 Years of the iPhone: An Interactive Timeline*, TIME (June 27, 2014), http://time.com/2934526/apple-iphone-timeline/.

171. *See Modernizing the Electronic Communications Privacy Act*, AM. CIVIL LIBERTIES UNION, http://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa (last visited Aug. 14, 2013).

172. S. REP. NO. 99-541, at 1 (1986).

173. *Id.* at 50.

174. 18 U.S.C. §§ 2701–2712 (2012).

175. Kerr, *supra* note 76, at 1211, 1213.

176. 18 U.S.C. § 2510 (2012) (defining an electronic communication service as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

companies) and remote computing service ("RCS")[177] providers (such as YouTube).

While the approaches mentioned in Parts III and IV primarily focus on compelling or gaining access to passwords from an individual, the analysis changes when a third-party service provider is subpoenaed—courts must consider the implications of the SCA. The SCA prevents a "provider" of communications from voluntarily disclosing communications or customer information to entities and individuals[178] and also *requires disclosure* of information in certain instances.[179] The SCA specifically requires a "provider of electronic communication service or remote computing service"[180] to disclose to the government "record[s] or other information pertaining to a subscriber to or customer of such service,"[181] when the governmental entity obtains a warrant or court order,[182] and to disclose the contents of the communications when the government complies with a specific framework.[183]

But the SCA does not explicitly mention disclosure of "passwords" or even define what constitutes a "record or other information pertaining to a subscriber or customer."[184] Even if some service providers classify passwords as "account information" alongside traditional forms of customer information, passwords may fall into the non-content provision of the SCA—if they lie anywhere within the SCA.[185] Without clear direction, lawyers, law enforcement, and third parties are left to guess whether the SCA covers disclosures of passwords by remote computing service or electronic communication service providers. This is not surprising given that electronic passwords did not exist when the ECPA and the SCA were enacted. But if passwords were found to be "electronic communications" (which "means

177. 18 U.S.C. § 2711 (2012) (defining a remote computing service as any service that provides the public with "computer storage or processing services by means of an electronic communications system").

178. Kerr, *supra* note 76, at 1223 ("Providers of ECS or RCS to the public ordinarily cannot disclose either content or noncontent information.").

179. *Id.* at 1224 ("One of the most fundamental distinctions in the SCA is the distinction between voluntary disclosure regulated by § 2702 and compelled disclosure regulated by § 2703.").

180. 18 U.S.C. § 2703(c)(1) (2012).

181. *Id.*

182. *Id.* § 2703(c)(1)(A)–(B) (stating that for certain types of investigations and when the government is only seeking basic subscriber information not subject to the scope of this Article, a governmental entity need only submit a formal written request).

183. *Id.* § 2703(a)–(b).

184. *See id.* § 2703(c)(1).

185. Contrast this to "contents," which "when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

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 photooptical system that affects interstate or foreign commerce"),[186] governmental entities could still obtain this information from third-party service providers with a warrant.[187]

Legal scholars should question the efficacy of the SCA in conjunction with the Fifth Amendment in the digital age and consider whether incriminating information should be further protected beyond the confines of the Fifth Amendment. If courts consider electronic passwords to be within the scope of the SCA, then governmental entities could use the SCA to compel disclosure of passwords from third-party providers (assuming that a court would find a service provider such as Google or Apple to be an ECS ("any service which provides to users thereof the ability to send or receive wire or electronic communications"[188])). If courts interpret the SCA this way, law enforcement could circumvent the Fifth Amendment by simply seeking information from third parties rather than the suspect.

VI. COMPELLING PASSWORDS FROM THIRD PARTIES

To date, only a few courts have ruled on whether individuals (or entities) can be forced to turn over passwords to their computer files.[189] Other courts

186. *Id.* § 2510(12).

187. *See id.* § 2703(a)–(b).

188. *Id.* § 2510(15). For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. S. REP. NO. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

189. In light of the rulings, only a few courts have specifically determined whether an individual is forced to turn over his password when law enforcement requests it. *See* United States v. Kirschner, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010) (compelling an individual's password would infringe on his Fifth Amendment incrimination privilege); Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614–15 (Mass. 2014) (holding that "entering an encryption key . . . would appear . . . to be a testimonial communication that triggers Fifth Amendment protection," but that based on the facts in the case, entering an encryption key was a foregone conclusion, and as such, "the act of decryption is not a testimonial communication that is protected by the Fifth Amendment"); Virginia v. Baust, No. CR14-1439, 2014 WL 6709960, at *3 (Va. Cir. Ct. 2014) (finding that "compelling Defendant to provide access through his passcode is both compelled and testimonial and therefore protected"). Other courts have skirted the Fifth Amendment protection and allowed disclosure of information without compelling disclosure of the actual password. *See In re* Under Seal, 749 F.3d 276, 293 (4th Cir. 2014) (finding no "basis upon which to challenge the Pen/Trap order" where petitioner failed to properly raise an argument about the district court's compulsion of encryption keys or the issue of plain error review); United States v. Fricosu, 841 F. Supp. 2d 1232, 1235, 1238 (D. Colo. 2012) (holding that defendant shall provide an unencrypted copy of her computer's hard drive to the government where the government sought a writ for the unencrypted contents); *In re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *1, *4 (D. Vt. Feb. 19, 2009) (directing the defendant to provide an unencrypted version of his

have wrangled with the question of whether individuals can be forced to turn over passwords to their social networking sites,[190] or whether individuals can be forced to unencrypt and produce the contents of their hard drives,[191] but the issue as to whether governmental entities can compel service providers to hand over users' passwords remains unresolved. As mentioned in Part I, the government is already requesting users' passwords from service providers, and "there are novel and serious [F]ourth and [F]ifth Amendment issues raised by a policy that would compel the use of recoverable encryption"[192] or some other form of third-party access to passwords.

A. SOLUTIONS FOR COMBATING COMPULSION OF PASSWORDS FROM SERVICE PROVIDERS

From the individual password holder's perspective, the government should not be able to get his password by subpoenaing a third party. But the Fourth and Fifth Amendments do not guarantee this prohibition and therefore do not adequately protect individuals when third parties are compelled to hand over passwords.

One possible solution to this problem is to require the government to demand an unencrypted copy of the protected data instead of the actual password.[193] Here, the government would only need to meet the search warrant requirements of the Fourth Amendment and use the SCA to obtain the information from a service provider, or subpoena the defendant to compel production of an unencrypted copy of the data (but only when it is a foregone conclusion that the incriminating evidence exists in the encrypted data).[194] However, this approach still has adverse privacy consequences. If

hard drive where the government's expert was unable to search a computer because of password-protection and where the subpoena had asked for "any passwords associated with the laptop").

190. *See, e.g.*, McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285, at *13 (Pa. Ct. Com. Pl. Sept. 9, 2010) (ordering plaintiff to "provide his Facebook and MySpace user names and passwords to counsel" for opposing parties' use).

191. *See In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1341 (11th Cir. 2012).

192. *Privacy in the Digital Age: Encryption and Mandatory Access: Hearing Before the Subcomm. on the Constitution, Federalism, and Prop. Rights of the Comm. on the Judiciary*, 105th Cong. 4 (1998) (statement of Sen. Russell D. Feingold), *available at* http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

193. *See Boucher II*, 2009 WL 424718, at *1; *see also Fricosu*, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012) (ordering defendant to deliver an unencrypted copy of the protected data instead of demanding the password).

194. *See In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d at 1346 (finding that it is not a foregone conclusion that the unencrypted contents contain incriminating evidence when it is not clear that the "[g]overnment knows whether any files

individuals are already concerned about the government accessing communications and communication records through government surveillance,[195] then what will come if the government begins compelling third parties to hand over the trove of information inside one's electronic device? Modern cellphones, with the "vast quantities of personal information" that they contain, could reveal "the privacies of life" for many Americans—not just of the cellphone's owner, but of others as well.[196] After all, many Americans conduct business via their phone, so a search of an individual's phone could include others' confidential information.[197] Thus a broader change is warranted, specifically one that takes into account both privacy and government concerns.

Another potential solution would be for service providers to not collect or store passwords in the first place. Most cellphone manufacturers and telecom providers do not currently collect or store passwords,[198] and any cellphone manufacturers who do collect this information should change direction and not collect or store passwords. An even stronger measure to ensure all service providers take the same action would be legislation prohibiting cellphone manufacturers from collecting and storing passwords. If this approach was adopted, governmental entities would not have the recourse currently available under the SCA to request passwords from service providers. Instead, they would have to obtain this information from individuals who could then invoke the Fifth Amendment. But as long as courts remain split on whether individuals are protected under the Fifth Amendment when the government attempts to compel their passwords, it remains unclear whether individuals' legal rights under the Fifth Amendment exist in this context. And it is unlikely that the government would enact legislation of this type given the government's reaction to Apple and

exist and are located on the hard drives" or that the individual is "even capable of accessing the encrypted portions of the drives").

195. *See, e.g.*, Michael Mimoso, *EFF Makes Case That Fifth Amendment Protects Against Compelled Decryption*, THREATPOST (Oct. 31, 2013, 2:08 PM), http://threatpost.com/eff-makes-case-that-fifth-amendment-protects-against-compelled-decryption/102767l/; *NSA Spying on Americans*, EFF, https://www.eff.org/nsa-spying/ (last visited Oct. 14, 2014).

196. Riley v. California, 134 S. Ct. 2473, 2485, 2495 (2014).

197. *See* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 627 (Mass. 1014) (Lenk, J., dissenting) (concluding "that the defendant could not be compelled to enter the decryption key . . . because of the possibility that the computers contain privileged information relating to the defendant's legal clients").

198. "Spokeswomen for Microsoft Corp. and Research In Motion Ltd. say their companies don't collect or store passwords." Angwin, *supra* note 2, at B4; *see also* Timberg, *supra* note 32 ("Apple once maintained the ability to unlock some content on devices for legally binding police requests but will no longer do so for iOS 8."); Timberg, *supra* note 28 (stating that the next generation of Google's Android operating system will encrypt data by default, thereby preventing anyone but the owner of the device from accessing the phone).

Google's announcements of engineering changes preventing the government from unlocking a user's electronic device.[199]

A third—and possibly most promising—solution would be for Congress to amend the ECPA. Congress could change the language of the ECPA and the SCA to allow third parties to invoke these statutes when compelled to hand over passwords, because the Supreme Court has made clear that third parties, even when agents of the suspect, cannot invoke the Fifth Amendment when they receive requests to hand over information that may incriminate the individual target of the investigation. Although Congress must balance the needs of law enforcement with the interests of privacy, this can still be accomplished if a caveat for password production is inserted into the SCA. A proposed amendment would state that third parties are not authorized to disclose an individual's password or encryption key to any other party, nor can they be required to hand over this information to the government unless specifically authorized by the individual account creator, in life-threatening situations, or in exigent circumstances as determined by a court.[200] However, given "[o]ur general preference to provide clear guidance to law enforcement through categorical rules,"[201] Congress would need to create clear standards for the exceptions. Moreover, this caveat would not prevent the government from compelling third parties to disclose the *content* of communications under the ECPA and the SCA. But it would prevent the government from accessing the "great deal of information"[202] that lies behind the passwords.[203]

B. COMPELLING PASSWORDS FROM EMPLOYERS

As more employers install monitoring software to track employees' every electronic move, the government may soon seek to compel employers to hand over their employees' passwords. Technologies such as keystroke logging make it possible for employers to monitor not only an employee's use of a computer, but also each and every one of their keystrokes.[204] In fact,

199. Timberg & Miller, *supra* note 33.

200. *See, e.g.*, *Riley*, 134 S. Ct. at 2494.

201. *Id.* at 2491.

202. *Id.*

203. It is also worth noting that a time may come when computers, cellphones, and other electronic devices use solely biometric information to "unlock" the device instead of a traditional password. Any changes to the laws to protect individuals' privacy rights should account for this broader concept of "passwords."

204. *See* Brahmana v. Lembo, No. C-09-00106 RMW, 2009 WL 1424438, at *3 (N.D. Cal. May 20, 2009) ("A key logger records each keystroke entered by the user of a particular computer."); *see also* United States v. Ropp, 347 F. Supp. 2d 831, 837–38 (C.D. Cal. 2004). According to the latest workplace monitoring and surveillance study, 45% of employers track content, keystrokes, and time spent at the keyboard, and 43% store and review

"[k]eystroke logging would provide employers the ability to obtain [an employee's] passwords if the employee accessed the site using an employer's computer."[205]

Although employers would likely not be considered an ECS[206] or RCS[207] provider for purposes of the ECPA and the SCA (though one could argue that employers provide their employees with the ability to send and receive electronic communications over their networks), in light of the advancing technology (keystroke logging) and the lagging ECPA, it is critical that Congress address this head on with an amendment to the ECPA. And given that keystroke logging has already been the subject of employment lawsuits,[208] employees and employers must understand their privacy rights should the government attempt to compel private employee information from employers under the basis that the employer is an ECS. Specifically, Congress should make clear that an employer (1) is not an ECS or RCS provider and (2) cannot be compelled to hand over employee data via the law of the ECPA and the SCA if the requested information is protected by the Fourth Amendment. Thus, an employer would have to first determine if the employee enjoys a legitimate expectation of privacy in the item being compelled before freely giving it over to law enforcement.

Under a traditional Fourth Amendment analysis, employees should still have a legitimate expectation of privacy in the passwords that they type into an employer-owned device, even if the employer uses keystroke logging software, because this type of software is usually installed in secret. But the

computer files. *The Latest on Workplace Monitoring and Surveillance*, AM. MGMT. ASS'N (Nov. 17, 2014), http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx.

205. Alexander Naito, Comment, *A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use*, 14 U. PA. J. CONST. L. 849, 864–65 (2012). *See also Brahmana*, 2009 WL 1424438, at *2, *3 (analyzing a situation in which an employer used monitoring tools, such as "Local Area Network Analyzers and keyloggers" to monitor the activities of their employees and in one case intercept an employee's password to his personal email account). But, keystroke logging "is a risky practice that may violate ECPA," and is extremely invasive. Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 315, 339 (2011). And employers might want "to revisit how they use keystroke monitoring or logging technology in light of [the N.D. Cal.] ruling." JACKSON LEWIS, *supra* note 115.

206. 18 U.S.C. § 2510 (2012) (defining electronic communication service as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

207. *Id.* § 2711 (defining remote computing service as "the provision to the public of computer storage or processing services by means of an electronic communications system").

208. *See, e.g.*, *Brahmana*, 2009 WL 1424438, at *3 (involving circumstances where the employer recorded the employee "entering his email password 'using software and hardware monitoring tools such as . . . key loggers'").

employee's reasonable privacy expectation would be compromised if an employer's policy specifically notifies the employee of the use of keystroke logging to track every word typed into an employer-owned device. Aside from this exception, however, passwords should not be treated as voluntarily given to employers in the same way that they are not voluntarily given to service providers. Although employers may have access to this information,[209] individuals probably do not assume that their employers need their passwords for any legitimate business purpose, nor do most employees know that employers can make permanent records of the passwords they enter (with of course the exception of a clearly-stated policy holding otherwise).[210]

VII. CONCLUSION

Increased access to rapidly changing technology necessitates Congressional action to ensure individuals' privacy rights remain protected as the Founders intended when they fought their own fight against unrestrained government invasion.[211] The ECPA and the SCA are outdated and do not reflect the privacy concerns that accompany the digital age. Moreover, the Fourth and Fifth Amendments do not adequately protect individuals from forcible and compulsory extortion of an individual's private passwords when the government compels them from a third party—and have even fallen flat in some instances when the government compels passwords from individuals. With all of this in mind, it is incumbent on Congress to consider how the government's recent tactics in compelling users' passwords from third parties flies directly counter to expectations of privacy and denies individuals a meaningful Fifth Amendment privilege when it comes to protecting their password-protected digital footprint.

209. JACKSON LEWIS, *supra* note 115.

210. *See* Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043 (D.C. Cir. 1978) (holding that "[t]o the extent an individual *knowingly* exposes his activities to third parties, he surrenders Fourth Amendment protections") (emphasis added).

211. *See* Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (noting that opposition to unrestrained searches "was in fact one of the driving forces behind the Revolution itself . . . for which the Founders fought").