UNLOCK YOUR PHONE AND LET ME READ ALL YOUR PERSONAL CONTENT, PLEASE: THE FIRST AND FIFTH AMENDMENTS AND BORDER SEARCHES OF ELECTRONIC DEVICES

KATHRYN NEUBAUER*

TABLE OF CONTENTS

*. Executive Notes Editor, *Southern California Law Review*, Volume 92; J.D., 2019, University of Southern California Gould School of Law; B.B.A., 2014, University of Michigan. My sincere gratitude to Professor Sam Erman for his invaluable feedback on early drafts of this Note as well as to Rosie Frihart, Kevin Ganley and all the editors of the *Southern California Law Review*. Thank you to Brian and my family—Mark, Diane, Elisabeth, Jennifer, Alison, Rebecca, Tony, Jason, Jalal, Owen, Evelyn, Peter and Manny—for all of their love and support. Finally, a special thank you Rebecca for reading and editing countless drafts, and to Jason for bringing to my attention this important issue.

On April 21, 2016, after spending five weeks travelling in Southeast Asia and participating in four Ultimate Frisbee tournaments, computer programmer Matthew Wright returned home by way of the Denver airport.[1] Upon his arrival from Tokyo, thirty-eight-year-old Mr. Wright, a resident of Colorado and a United States citizen, was directed by Customs and Border Protection ("CBP") officers to a separate inspection area where they asked

1. Deb Riechmann, *Lawsuit Targets Searches of Electronic Devices at U.S. Border*, DENVER POST (Sept. 13, 2017, 9:29 AM), https://www.denverpost.com/2017/09/13/lawsuit-targets-electronic-devices-search; *Matt Wright*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/bio/matt-wright (last visited Aug. 25, 2019). Please note that his introductory account is based predominately on allegations made in a complaint. Therefore, whether these allegations did in fact happen is currently unclear.

Mr. Wright to unlock a laptop they found in his bag.[2] When Mr. Wright refused to unlock his device, a CBP officer informed him that CBP would seize his device and cautioned that it could take up to a year for his device to be returned.[3]

After Mr. Wright continued to resist the CBP officer's direction to unlock his laptop, the CBP not only confiscated the laptop and his phone but also his camera, which had no locking feature.[4] Given the necessity of a computer and phone for his job as a computer programmer, shortly after the incident, Mr. Wright spent $2419.97 to replace the laptop and phone confiscated by CBP officers.[5] Mr. Wright could not support himself without his devices, which were confiscated without any warrant or reasonable suspicion.[6] Pursuant to the Freedom of Information Act, the government attempted to copy everything on Mr. Wright's laptop using MacQuisition software and extracted data from SIM cards located in Mr. Wright's phone and camera.[7] Fifty-six days later, Mr. Wright's devices were returned to him.[8] According to the CBP records, no "derogatory" information was found on any of the devices.[9]

Mr. Wright is one of ten United States citizens who filed similar suits against the government in September 2017.[10] Of these individuals, most are people of color, many are Muslim, some were traveling for business, some were traveling for personal reasons, some had their devices detained for weeks and others had their devices returned months later.[11] All of the individuals, however, were United States citizens who were reentering their own country, and all searches of their devices were conducted without a warrant and without any specific reasonable suspicion.[12]

2. Amended Complaint at 35, Alasaad v. Duke, No. 1:17-cv-11730-DJC (D. Mass. Sept. 13, 2017); *Matt Wright*, *supra* note 1.

3. Amended Complaint, *supra* note 2, at 13; *Matt Wright*, *supra* note 1.

4. Amended Complaint, *supra* note 2, at 13; *Matt Wright*, *supra* note 1.

5. Amended Complaint, *supra* note 2, at 13–14; *Matt Wright*, *supra* note 1.

6. *Alasaad v. Nielsen: Plaintiffs' Stories*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/alasaad-vs-duke-bios (last visited Aug. 25, 2019).

7. *Id.*; Amended Complaint, *supra* note 2, at 10–11.

8. Amended Complaint, *supra* note 2, at 13.

9. *Id.* at 36.

10. *Id.* at 1.

11. *Alasaad v. Nielsen*, BRENNAN CTR. FOR JUST. (Feb. 5, 2018), https://www.brennancenter.org/legal-work/alasaad-v-nielsen.

12. Amended Complaint, *supra* note 2, at 2; *Alasaad v. Nielsen: Plaintiffs' Stories*, *supra* note 6.

INTRODUCTION

Until January 2018, under the border search exception, CBP officers were afforded the power to search any electronic device without meeting any standard of suspicion or acquiring a warrant.[13] The border search exception is a "longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained . . . ."[14] It provides that suspicionless and warrantless searches at the border are not in violation of the Fourth Amendment merely because searches at the border are "reasonable simply by virtue of the fact that they occur at the border . . . ."[15] The CBP, claiming that the border search exception applies to electronic devices, searched more devices in 2017 than ever before, with approximately a 60 percent increase over 2016 according to data released by the CBP.[16] These "digital strip searches"[17] violate travelers' First, Fourth, and Fifth Amendment rights. With the advent of smartphones and the expanded use of electronic devices for storing people's extremely personal data, these searches violate an individual's right to privacy. Simply by travelling into the United States with a device linked to such information, a person suddenly—and, currently, unexpectedly—opens a window for the government to search through seemingly every aspect of his or her life. The policy behind these searches at the border does not align with the core principles behind our longstanding First and Fifth Amendment protections, nor does it align with the policies behind the exceptions made to constitutional rights at the border in the past.

In order to protect the privacy and rights of both citizens and noncitizens

13. *See* Opinion, *Border Agents Can Look at Everything on Your Cellphone*. *Congress Should Change That*, WASH. POST. (Apr. 12, 2017), https://www.washingtonpost.com/opinions/border-agents-can-look-at-everything-on-your-cell-phone-congress-should-change-that/2017/04/12/5e95b2ec-1bc7-11e7-855e-4824bbb5d748_story.html?utm_term=.f3e95bcc9942; Vanessa Romo & Joel Rose, *U.S. Customs and Border Protection Sets New Rules for Searching Electronic Devices*, NAT'L PUB. RADIO: THE TWO-WAY (Jan. 5, 2018, 8:40 PM), https://www.npr.org/sections/thetwo-way/2018/01/05/576139303/u-s-customs-and-border-patrol-sets-new-rules-for-searching-electronic-devices.

14. United States v. Ramsey, 431 U.S. 606, 621 (1977).

15. *Id.* at 616.

16. Press Release, U.S. Customs & Border Prot., CBP Releases Updated Border Search of Electronic Devices Directive and FY17 Statistics (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and#. During the fiscal year 2017, a total of 30,200 travelers' electronic devices were searched, and in the fiscal year 2016, a total of 19,051 devices were searched. *Id*. This was approximately a 58% increase in searches. *See id.*

17. Michelle Kaminsky, *'Stranger Things' at Border Control: Electronic Device Searches Increasingly Common*, FORBES (Oct. 30, 2017, 12:59 PM), https://www.forbes.com/sites/michellefabio/2017/10/30/stranger-things-at-border-control-electronic-device-searches-increasingly-common/#18ccd86c553c.

entering the United States, the procedures concerning electronic device searches need to be rectified. For instance, the border search exception should not be applied to electronic devices the same way it applies to other property or storage containers, like a backpack. One is less likely to expect privacy in the contents of a backpack than in the contents of a password- or authorization-protected devices—unlike a locked device, a backpack can be taken, can be opened easily, can fall open, and also has been traditionally subjected to searches at the border. Moreover, there are many reasons why electronic devices warrant privacy. First, the combination of information on an electronic device can tell a viewer much more than the limited materials held inside a backpack. In fact, the contents of a device can reveal every aspect of its user's life—calendars, the phone number of his or her dry cleaner, the last place set in a navigation system, the number of steps taken the prior Wednesday, and the Instagram photograph shot this morning. The combination of all this information can reveal much more than a packed bag carried across the border.

Second, a device stores data from much further back in time. For instance, while someone may hold in a backpack a notepad telling him or her to call back an individual, a phone will have stored a record of all communications made with the individual since owning the device (or even longer if the device has downloaded information from a previous device). A person does not expect this information to be readily available, and many forget it is even in his or her pocket. Overall, an individual's expectation of privacy in a locked personal device overwhelmingly outweighs the CBP's prerogative to search items coming into the country.

If, however, we assume the border search exception continues to extend to these devices, then the Fifth Amendment should, at the very least, protect travelers from having to unlock their devices themselves for officers. Some lower courts have established that the Fifth Amendment protects passwords and encryptions from being compelled from a person, even when he or she is not subject to a criminal investigation.[18] By that same principle, biometric authorizations, like unlocking a phone with a fingerprint or face recognition, should be protected from compulsion by CBP officers. With the introduction of fingerprint authorization and the growing popularity of facial recognition, there is an illusion that an individual's phone is more secure than ever before; however, the Fifth Amendment, as currently applied, does not protect against

18. *E.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010). *Contra In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *9–10 (D. Vt. Feb. 19, 2009).

the government compelling an individual to unlock a device using biometric authorization and actually makes devices less protected from government invasion than a traditional password. This should not be the case. The Fifth Amendment should protect all devices equally, whether the device is opened by a password or biometric authorization. Travelers should be able to invoke the Fifth Amendment at the border and prevent unfettered access to their devices by easily refusing to supply a password or biometric authorization to unlock their device.

Lastly, in the case that Fourth and Fifth Amendment protections do not bar searches of electronic devices at the border, the First Amendment should preclude any such searches (even "basic searches"[19]) conducted without reasonable suspicion. Travelers should feel safe to say, read, share, and associate, and to do so anonymously without fear—which is at the core of the First Amendment's protections. Searches as currently conducted violate the First Amendment and precedent only allows such piercing of the First Amendment when there is a compelling state interest that outweighs the cost of impairing free speech, and there is no less restrictive method of meeting that state need. Here, the cost is much too high, and lack of a standard of suspicion is more restrictive than needed to meet any state security interest at the border.

This Note will briefly discuss the Fourth Amendment and the border search exception but will focus on the First and Fifth Amendment violations taking place under current procedures. This Note will also suggest policy changes in order to protect these rights during border searches of electronic devices.

I. BACKGROUND

A. BRIEF HISTORY OF THE CBP AND BORDER SEARCHES

In July 1789, President George Washington signed an Act that gave the government the "full power and authority" to search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise

19. According to the most recent CBP Directive on searches of electronic devices issued in January 2018, a "basic search" of an electronic device is any search that is not considered an "advanced search." An "advanced search" is defined as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." U.S. CUSTOMS & BORDER PROT., DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES 4–5 (2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf [hereinafter U.S. CUSTOMS & BORDER PROT., 2018 DIRECTIVE].

subject to duty shall be concealed . . . ."[20] Thus, a limitation to privacy at the border began early in United States history. Today, CBP officers have the authority to

> examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board, and to this end may hail and stop such vessel or vehicle, and use all necessary force to compel compliance.[21]

The CBP, along with other agencies, operate under the "border search exception" to the Fourth Amendment's protections, which allows border officers to conduct routine searches without either a warrant or probable cause.[22] The Supreme Court has held that these border searches are considered "reasonable simply by virtue of the fact that they occur at the border . . . ."[23] and this extends "not only at the border itself, but at its functional equivalents as well," including airports.[24] The rationale behind this exception is that the United States has the longstanding right and prerogative to examine persons and property entering the country.[25] This justification harkens back to an 1886 case, *Boyd v. United States*, in which the Supreme Court recognized this exception to the Fourth Amendment in part because the law "was passed by the same [C]ongress [that] proposed for adoption the original amendments to the [C]onstitution, [and] it is clear that the members of that body did not regard searches and seizures of this kind as 'unreasonable' . . . ."[26] Even though the law granting the search in *Boyd* was found unconstitutional on other grounds, future courts have almost

20. Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43.

21. 19 U.S.C. § 1581(a) (2018).

22. United States v. Pickett, 598 F.3d 231, 234 (5th Cir. 2010). A search of an inanimate object is generally considered "routine" absent a showing that the technique used to conduct the search was too intrusive. United States v. Molina-Tarazon, 279 F.3d 709, 713 (9th Cir. 2002). It has been assumed by various courts that manual searches of electronic devices are now searches as opposed to nonroutine searches that would require suspicion or a warrant. United States v. Cotterman, 709 F.3d 952, 962–68 (9th Cir. 2013). However, recently, a circuit split has arisen about whether forensic searches of devices are routine. *Compare* United States v. Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018) (deciding that, especially in light of *Riley v. California* and the invasiveness of a search of a digital phone, there must be individualized suspicion to perform a forensic search), *with* United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) (holding that, because a forensic search of an electronic device is not as intrusive as a strip search or x-ray, even though it is somewhat intrusive, it is just a search of property and no suspicion is required).

23. United States v. Ramsey, 431 U.S. 606, 616 (1977).

24. Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973).

25. *Ramsey*, 431 U.S. at 616.

26. Boyd v. United States, 116 U.S. 616, 623 (1886). In *Boyd*, the law was found unconstitutional and void on Fifth Amendment grounds, however. The law required the compulsion of evidence to be used against the claimant, which the Court found to be unconstitutional. *Id.* at 618.

universally upheld this idea as a justification for warrantless border searches.[27]

Since *Boyd*, the Court has continually used both the temporal nexus of the original customs laws, the black and white text of the Constitution, and the justification that a sovereign needs to protect itself to rationalize warrantless searches at the border.[28] By the 1970s to the 1980s, the Supreme Court began to expand the border search exception to include searches at the border conducted without any suspicion.[29]

However, there are some limitations to warrantless searches at the border. The Supreme Court has noted that although some privacy rights are not protected in the same way at the border as they are anywhere else, these protections are properly pierced only if they are outbalanced by the need to protect the United States.[30] For instance, many courts have found that intrusive searches of a person's body at the border not only require suspicion but also require a strong indication or suggestion of criminal activity.[31] Still, the CBP has acted as if there is no such suspicion requirement for electronic devices coming through the border.

B. ELECTRONIC DEVICE SEARCHES BEFORE JANUARY 2018

In the early 2000s, the CBP began to extend the border search exception to electronic devices carried at the border.[32] After years of such searches, in 2009, the CBP issued a directive entitled "Border Searches of Electronic Devices Containing Information" ("2009 Directive").[33] The 2009 Directive

27. Gregory T. Arnold, *Criminal Law—Bordering on Unreasonableness?: The Third Circuit Again Expands the Border Search Exception in* United States v. Hyde, 40 VILL. L. REV. 835, 843 (1995).

28. *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 537–39 (1985); *Ramsey*, 431 U.S. at 616–20.

29. Sid Nadkarni, Note, *"Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices*, 61 UCLA L. REV. 146, 161 (2013).

30. United States v. Cotterman, 709 F.3d 952, 960 (9th Cir. 2013).

31. *E.g.*, Rivas v. United States, 368 F.2d 703, 710 (9th Cir. 1966) (discussing the validity of border searches and seizures by customs officers). In relatively recent cases, the courts have held that, for a body search, CBP officers must have more than even just suspicion but also "clear indication" or "plain suggestion" of criminal activity. *E.g.*, Henderson v. United States, 390 F.2d 805, 808 (9th Cir. 1967) (quoting *Rivas*, 368 F.2d at 710). These are seen as non-routine searches, however, as opposed to electronic searches that are deemed to be routine.

32. Masood Farivar, *At US Border, Dramatic Spike in Searches of Phones, Electronic Devices*, VOA (Oct. 28, 2017, 2:21 AM), https://www.voanews.com/a/us-border-spike-in-searches-of-phones-electronic-devices/4090013.html.

33. U.S. CUSTOMS & BORDER PROT., DIRECTIVE NO. 3340-049, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION 1 (2009), https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf [hereinafter U.S. CUSTOMS & BORDER PROT., 2009 DIRECTIVE].

granted CBP officers the authority, "with or without individualized suspicion," to "examine electronic devices and . . . review and analyze the information encountered at the border . . . ."[34] The CBP could then detain the electronic devices for up to five days and could easily request extensions for further detainment.[35] The CBP could also retain the electronic device or copied information if it is determined that there is probable cause; in other words, that the device likely "contains evidence of or is the fruit of a crime that CBP is authorized to enforce" or it must destroy the copied information.[36] However, even without probable cause, the CBP could retain information "relating to immigration, customs, and other enforcement matters . . . ."[37] Further, the 2009 Directive allowed the CBP "to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy."[38]

According to the American Civil Liberties Union ("ACLU"), if travelers decline to hand over passwords or unlock their devices, CBP officers will threaten travelers with longer detainment times or to keep their devices.[39] For instance, in October 2016, a Canadian photojournalist en route to cover the Dakota Access oil pipeline protests was detained by officers who forced him to unlock his phones so that they could look through his photographs.[40] The journalist refused, claiming that "[g]iving up the contents of his private phone would be akin to a doctor giving up confidential patient information . . . ."[41] He continued to refuse even after officers seized his two phones (which were returned with signs that the SIM cards had been replaced) and denied him entry to the United States.[42]

CBP officers often intimidate travelers into handing over their devices and passwords. CBP officers' uniforms, threatening weapons on their

34. *Id.* at 3.
35. *Id.* at 4–5.
36. *Id.* at 7.
37. *Id.*
38. *Id.*
39. Hugh Handeyside & Esha Bhandari, *Warrantless Border Searches of Smartphones Are Skyrocketing. We're Suing to Stop Them*., AM. CIV. LIBERTIES UNION (Sept. 13, 2017, 11:00 AM), https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/warrantless-border-searches-smartphones-are.
40. Daniel Victor, *Canadian Journalist's Detention at U.S. Border Raises Press Freedom Alarms*, N.Y. TIMES (Dec. 2, 2016), https://www.nytimes.com/2016/12/02/business/media/canadian-journalists-detention-at-us-border-raises-press-freedom-alarms.html.
41. *Id.*
42. *Id.*

persons, and practices—such as seizing passports, detaining travelers in small rooms, using travelers' connecting travel plans to hurry them into handing over passwords and information, and threatening of the indefinite seizure of personal devices—all coerce travelers to comply with CBP requests to unlock devices so that officers can search through the contents.[43] In one incident in 2012, a father, his two American children, and his wife were detained for five hours while CBP officers coerced their passwords and began looking through private emails and Facebook accounts.[44] When the father asked how much longer the search would take, the officers put him in handcuffs.[45]

Additionally, if a United States citizen or legal permanent resident refuses to hand over his or her password or unlock his or her device, the CBP can keep the device but cannot deny entry to the United States; however, if a noncitizen refuses to unlock his or her device for the officers, he or she may be denied entry to the United States altogether.[46]

Due to a higher sense of privacy incidental to a locked electronic device, the practice of examining electronic devices at the border unnecessarily leaves travelers entering the United States feeling violated. The Supreme Court, however, has yet to specifically address the search of electronic devices at the border and rule on its constitutionality. Meanwhile, the number of devices being searched at the border is increasing.[47]According to the CBP itself, in 2015 the devices of 8,503 people (0.002% of international travelers processed by the CBP) were searched.[48] In 2016, the number of devices that were searched increased to 19,033 (0.005%), and in the first half of 2017, 14,993 (0.008%) devices had already been searched.[49] So, while in 2015 CBP seized roughly 23 electronic devices per day, by the end of 2017 it

43. *See* Adam Schwartz & Sophia Cope, *Pass the Protecting Data at the Border Act*, ELECTRONIC FRONTIER FOUND. (Oct. 13, 2017), https://www.eff.org/deeplinks/2017/10/pass-protecting-data-border-act.

44. Charlie Savage & Ron Nixon, *Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011*, N.Y. TIMES (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/us/politics/us-border-privacy-phone-searches.html.

45. *Id.*

46. Stephanie Lacambra, *The Bill of Rights at the Border: Fourth Amendment Limits on Searching Your Data and Devices*, ELECTRONIC FRONTIER FOUND. (Apr. 3, 2017), https://www.eff.org/deeplinks/2017/04/bill-rights-border-fourth-amendment-limits-searching-your-data-and-devices.

47. *See* Press Release, U.S. Customs & Border Prot., CBP Releases Statistics on Electronic Device Searches (Apr. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0.

48. *Id.*

49. *Id.*

increased to roughly 82 devices seized per day.[50] The CBP defended the increase in searches and its policy as aligning with its "mission to protect the American people and enforce the nation's laws in this digital age" and the searches' effectiveness in "combating terrorist activity, child pornography, violations of export controls, intellectual property rights violations, and visa fraud."[51]

C. JANUARY 2018 CHANGES

In January 2018, perhaps in response to the various complaints and also to comply with the decisions made by federal courts, the CBP issued a new directive entitled "Border Search of Electronic Devices" (the "2018 Directive"), which superseded the pervious 2009 Directive.[52] The 2018 Directive clarified or changed various practices that had been employed by the CBP prior to 2018.[53]

First, the 2018 Directive distinguished between "basic" and "advanced" searches. The 2018 Directive defines a "basic search" as any search of an electronic device that is not an "advanced" search.[54] An "advanced search" includes "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to the device, but to review, copy, and/or analyze its contents."[55] To conduct an advanced search, there must be reasonable suspicion of activity in violation of the law or a national security concern.[56] The 2018 Directive goes on to say there are many factors that can create reasonable suspicion and provides an example but does not give standards for what rises to "reasonable suspicion" or a "national security concern."[57] Similar to the previous directive, the 2018 Directive does not require any standard of suspicion for conducting a basic search.[58] This means that CBP officers can still go through a smartphone to read personal emails and texts, look at personal photographs, and much more without any suspicion whatsoever.

50. Stephen Dinan, *U.S. Border Guards Increase Searches of Electronic Devices*, WASH. TIMES (Apr. 11, 2017), http://www.washingtontimes.com/news/2017/apr/11/us-border-guards-up-searches-electronic-devices.

51. Press Release, U.S. Customs & Border Prot., *supra* note 47.

52. U.S. CUSTOMS & BORDER PROT., 2018 DIRECTIVE, *supra* note 19, at 12.

53. *Id.*

54. *See id.* at 4.

55. *Id.* at 5.

56. *Id.*

57. *Id.*

58. *Id.* at 4.

Second, the 2018 Directive reinforced the pronouncement that CBP officers should refrain from searching through any information that is not locally stored on the device. The 2018 Directive instructs officers to refrain from "intentionally us[ing] the device to access information that is solely stored remotely" and to either request that travelers disable the device's connection to the network or disable the connectivity themselves.[59]

Third, travelers are not "obligated to present [an] electronic device and the information contained therein in a condition that allows inspection of the device and its contents."[60] If CBP officers do not obtain a password, they have the power to detain the device.[61] This is a significant change from the 2009 Directive under which the CBP did not have this explicit authority to make travelers hand over unlocked devices, although it was its common practice.

Fourth, the 2018 Directive set out new procedures for handling privileged information.[62] Now, when any information found to be or asserted to be protected by attorney-client privilege is found, CBP officers will contact the CBP Associate/Assistant Chief Counsel office who will employ a "Filter Team" to segregate information.[63] However, other privileged information, including medical records and journalist's work, are only vaguely protected by "any applicable federal law and CBP policy" without any additional information.[64]

D. THE CLOUD, PRIVILEGED INFORMATION, PERSONNEL, AND THE ISSUES FACING 2018

While the ACLU called the new suspicion standard for advanced searches an improvement, there are still many issues unresolved and unconstitutional.[65] One such issue is whether the CBP can access just data that is stored remotely or also data stored on the cloud. The 2009 Directive gave the CBP the authority to search "information encountered at the border" without qualifying whether it can access data that is not locally stored through a device.[66] However, in response to a letter sent by United States Senator Ron Wyden in June 2017, the CBP claims that "border searches

59. *Id.*
60. *Id.* at 6.
61. *Id.*
62. *Id.* at 5–6.
63. *Id.* at 5.
64. *Id.* at 6.
65. Romo & Rose, *supra* note 13.
66. U.S. CUSTOMS & BORDER PROT., 2009 DIRECTIVE, *supra* note 33, at 3.

conducted by CBP do not extend to information that is located solely on remote servers."[67] The 2018 Directive did clarify by explicitly saying "[o]fficers may not intentionally use the device to access information that is solely stored remotely."[68] Yet, it is often difficult when looking through a device to see what applications have only locally stored information and what information is being pulled from the cloud or remote server.[69] To combat this, the 2018 Directive directs officers to either request that individuals disconnect their devices from any network (for instance, putting a phone into "airplane mode") or disable the network connection to their devices themselves in certain situations.[70] However, this is not enough to protect the breadth information not remotely stored. Information is constantly flowing between the phone, the internet, and the cloud.[71] An officer may fail to direct you to turn off cellular data or Wi-Fi connection because it is easy to overlook. A look through a phone that has been disconnected still shows cloud information, but it may not be interactive.

Secondly, access to privileged and sensitive information, such as attorney-client or doctor-patient correspondence and documentation, or delicate personal information causes concern. While privileged information is not per se exempt from any border search, both the CBP and Immigration and Customs Enforcement ("ICE") have set out special procedures in dealing with devices known to contain such sensitive materials.[72] The 2018 Directive lays out a process to handle attorney-client information.[73] However, the directive does not give a specific policy with regard to other sensitive information, such as medical records, journalists' work, and confidential business information.[74] The directive states "business or commercial information" should be treated as "business confidential information . . . ."[75] However, these policies do not seem to protect privileged information because they can still be accessed by officers.

Before the 2018 Directive's announcement, the American Bar Association ("ABA") publicly pleaded with the CBP to change these

67. Letter from Kevin McAleenan, Nominee for Comm'r of U.S. Customs & Border Prot., to Ron Wyden, U.S. Senator (June 20, 2017), https://www.aila.org/infonet/cbp-border-searches-of-personal-electronic-devices (answering questions posed by the senator).

68. U.S. CUSTOMS & BORDER PROT., 2018 DIRECTIVE, *supra* note 19, at 4.

69. Riley v. California, 573 U.S. 373, 398 (2014).

70. *Id.*

71. *Id.*

72. Abidor v. Napolitano, 990 F. Supp. 2d 260, 266–67 (E.D.N.Y. 2013).

73. U.S. CUSTOMS & BORDER PROT., 2018 DIRECTIVE, *supra* note 19, at 5–6.

74. *Id.* at 6.

75. *Id.*

policies, especially as it relates to attorneys traveling with attorney-client privileged information.[76] The ABA asked that the current policy be amended to allow only physical inspections of devices claiming to have privileged or confidential client information and to disallow any reading, duplicating, seizing, or sharing of any contents.[77] The 2018 directive falls short of these hopes. The ABA now is urging the CBP and other agencies to adopt a policy that would require officers to "obtain a subpoena based on reasonable suspicion or a warrant supported by probable cause before searching the contents of lawyer electronic devices."[78]

Additionally, the Trump administration has put a lot of weight behind the CBP by both increasing the number of CBP searches and its manpower.[79] President Trump has promised to hire fifteen thousand new CBP officers and immigration personnel.[80] However, given the high standards required for employment as CBP officers combined with the high attrition rate, the Department of Homeland Security claims that it "would have to vet 750,000 applicants to find 5,000 qualified personnel."[81]

Still, President Trump, by executive order in January 2017, required the hiring of five thousand additional CBP agents.[82] Two years after that executive order, there were two thousand more vacancies in the CBP than before Trump signed the order.[83] Efforts to fill those positions have included

76. Rhonda McMillion, *The ABA Urges Homeland Security to Revise Procedures for Searching Lawyers' Electronic Devices*, AM. B. ASS'N. J. (Aug. 1, 2017, 12:35 AM), http://www.abajournal.com/magazine/article/border_searches_confidential_client_info.

77. *Id.*

78. Lee Rawles, *Traveling Lawyers Get New Protections in Device Searches at Border*, AM. B. ASS'N. J. (Jan. 25, 2018, 11:01 AM) (citation omitted), http://www.abajournal.com/news/article/new_guidelines_for_electronic_device_searches_at_us_borders_will_impact_att. The ABA Standing Committee on Ethics and Professional Responsibility gave advice to lawyers, given the current CBP practices, including to (1) consider leaving devices at home and not traveling with them; (2) consider buying disposable or inexpensive devices and storing only the information you need while traveling; (3) be cautious of the confidential information you have stored in the device and be knowledgeable that a simple "delete" does not always fully remove data from the device; and (4) place devices in "airplane" mode, fully power down, and lock your devices when approaching the border inspection area. *Id.*

79. Lisa Rein, *Trump Plan to Hire 15,000 Border and Immigration Personnel Isn't Justified, Federal Watchdog Says*, WASH. POST (Aug. 2, 2017), https://www.washingtonpost.com/politics/trump-plan-to-hire-15000-border-and-immigration-personnel-isnt-justified-federal-watchdog-says/2017/08/02/c9345136-77a1-11e7-8839-ec48ec4cae25_story.html?utm_term=.f6acfd89f679.

80. *Id.*

81. *Id.*

82. Border Security and Immigration Enforcement Improvements, 82 Fed. Reg. 8793 (Jan. 25, 2017).

83. Molly O'Toole, *Trump Ordered 15,000 New Border and Immigration Officers—But Got Thousands of Vacancies Instead*, L.A. TIMES (Jan. 27, 2019, 3:00 AM), https://www.latimes.com/politics/la-na-pol-border-patrol-hiring-20190126-story.html.

trying to use social media, reaching out to students, waiving polygraph tests for some applicants, and speeding up the hiring process from 469 days in January 2016 to 165 days in March 2017.[84] There is potential that the lowering of standards and quicker procedures could lead to the hiring of unqualified or corrupt CBP officers.[85]

II. BRIEF DISCUSSION ON THE FOURTH AMENDMENT AND ELECTRONIC DEVICE SEARCHES AT THE BORDER

A. INTRODUCTION

The Fourth Amendment gives people "[t]he right . . . to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," states that "no Warrants shall [be issued without] probable cause,"[86] and was implemented to protect people's privacy and to limit the reach of the government.[87] The Fourth Amendment, however, is not absolute. As discussed previously, the border search exception gives the CBP the right to conduct warrantless searches at the border. One principle behind the border search exception is that people have lower expectances of privacy in their personal effects when crossing the border.[88] In 2004, the Supreme Court "noted that the expectation of privacy is less at the border than it is in the interior."[89] Although this diminished sense of privacy is true for most travelers regarding their backpacks or suitcases carried across the border, the

84. Rafael Carranza, *CBP: Trump's 5,000 Border Patrol Hires Won't Mean Lower Standards*, AZCENTRAL.COM, http://www.azcentral.com/story/news/politics/border-issues/2017/03/15/cbp-no-plans-lower-border-patrol-hiring-standards/99227430 (last updated Mar. 16, 2017, 1:33 PM); Joseph Tanfani, *In January, President Trump Vowed to hire 5,000 New Border Patrol Agents. It Never Happened*, L.A. TIMES (Aug. 18, 2017, 4:10 PM), https://www.latimes.com/politics/la-na-border-security-20170818-story.html. After a series of corruption cases, in 2012, the CBP was directed by congress to conduct polygraph tests on applicants. Greg Moran, *Trump's Plan to Rapidly Expand Border Patrol Comes with Big Risks*, L.A. TIMES (Mar. 13, 2017, 5:00 AM), http://www.latimes.com/local/lanow/la-me-border-patrol-20170313-story.html; *see also* Tal Kopan, *Best CBP Estimates Say Hiring Could Take Decade*, CNN, http://www.cnn.com/2017/03/07/politics/border-agents-cbp-hiring-slow/index.html (last updated Mar. 8, 2017, 1:58 AM).

85. Moran, *supra* note 84.

86. U.S. CONST. amend. IV.

87. Messerschmidt v. Millender, 565 U.S. 535, 568 (2012) (Sotomayor, J., dissenting) ("The Fourth Amendment was adopted specifically in response to the Crown's practice of using general warrants and writs of assistance to search 'suspected places' for evidence of smuggling, libel, or other crimes." (quoting Boyd v. United States, 116 U.S. 616, 625–26 (1886))).

88. Given the notoriety of searches at the border, travelers are on notice of the type of searches that are conducted and have a diminished expectation of privacy. *See* Paul S. Rosenzweig, *Functional Equivalents of the Border, Sovereignty, and the Fourth Amendment*, 52 U. CHI. L. REV. 1119, 1133 (1985).

89. United States v. Flores-Montano, 541 U.S. 149, 154 (2004) (citation omitted).

same cannot be said regarding their electronic devices and the information that they do not realize they are carrying on their person.[90]

Electronic devices today hold deeply personal information, in large volumes; people expect that the collection of this data is private and stored beyond the reach of someone who may hold the physical storage device.[91] In recent years, various courts have wrestled with whether electronic searches are reasonable searches at the border.[92] For instance, a person may hold in a bag private items such as a journal, a notebook, makeup, and other such items that he or she would feel are personal, but on an electronic device, a search can reveal a person's spending habits, communication over email thought to never be seen by anyone other than the sender and intended receiver, medical records, and social media accounts and information.[93] Also, the combination of information inside a small device gives access to one's entire life beyond one's expectation of what information is actually accessible within the device.[94]

The smartphone is almost an extension of the human mind to many. The phone stores personal thoughts, business, friendly and romantic relationships, the memory through history of usage, the locations where the owner has been and is planning to go, the preferences and affiliations of the user, and much more.[95] Justice Roberts commented on how modern phones have become "a pervasive and insistent part of daily life" and pointed out, perhaps humorously, that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[96] Simply put, electronic devices today cannot be treated as ordinary objects subjected to ordinary search procedures.

B. BORDER SEARCHES OF ELECTRONIC DEVICES AND THE FOURTH AMENDMENT'S HISTORY

The border search doctrine has generally been accepted to extend to electronic devices at the border. Specifically, *manual* searches can be

90. *See* Editorial, *Border Agents Want to Search a Traveler's Laptop and Phone? Get a Warrant*, L.A. TIMES (Sept. 19, 2017, 4:00 AM), http://www.latimes.com/opinion/editorials/la-ed-laptops-search-20170919-story.html.

91. Riley v. California, 573 U.S. 373, 393–97 (2014).

92. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 966–68 (9th Cir. 2013); United States v. Ickes, 393 F.3d 501, 502 (4th Cir. 2005).

93. *Riley*, 573 U.S. at 393–97.

94. *Id.*

95. *Id.*

96. *Id.* at 385.

suspicionless and warrantless; however, it is unclear whether courts will require reasonable suspicion when conducting a more invasive *forensic* search of devices.[97]

In 2000, John Ickes drove to the Canadian-American border.[98] CBP officers searched his van and discovered a computer and seventy-five disks containing child pornography.[99] Ickes claimed that the search violated his First and Fourth Amendment rights, but the Fourth Circuit held that the search was constitutional under the border search exception.[100] The Fourth Circuit determined that the statutory language, "the broader context of the statute as a whole," and the historical context authorized CBP officers to conduct a search of the computer and disks.[101] Furthermore, the Fourth Circuit refused to create a First Amendment carve out to the border search exception, claiming the issues of such a carve out could impede the protection of our country.[102]

Similarly, in 2005, Michael Arnold was traveling from the Philippines and arrived at Los Angeles International Airport, where a CBP officer selected him for additional questioning.[103] In Arnold's luggage he carried with him a laptop computer, a separate hard drive, six compact discs, and a USB drive.[104] Arnold was asked to turn on his laptop computer, and a CBP officer saw two folders on the desktop screen and asked Arnold to open the folders.[105] A CBP officer viewed a photo depicting nude women, which prompted him to call his supervisors who conducted an examination of Arnold's computer.[106] They found images of child pornography, and he was later charged with three counts relating the possession of these materials.[107] In the Ninth Circuit appeal that followed, *United States v. Arnold*, Arnold argued reasonable suspicion was needed to search his computer, and the evidence should be suppressed.[108] Arnold specifically argued that laptops were "fundamentally different" from baggage and containers brought

97. *See, e.g.*, *Cotterman*, 709 F.3d at 966–68.

98. United States v. Ickes, 393 F.3d 501, 502 (4th Cir. 2005).

99. *Id.* at 502–03.

100. *Id.* at 503.

101. *Id.* at 504 (quoting Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997)).

102. *Id.* at 506. The Fourth Circuit claimed that a First Amendment exception would create "headaches," would create protections for "terrorists plans," "which are inherently 'expressive,'" and would thus divert the CBP from its "charge of policing our borders." *Id.*

103. United States v. Arnold, 533 F.3d 1003, 1005 (9th Cir. 2008).

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.* at 1005–06.

108. *Id.* at 1006.

through the border and were in fact more similar to a home or human mind than a suitcase.[109] However, the Ninth Circuit, agreeing with the Fourth Circuit's decision in *Ickes*, held that the border search exception doctrine applied and the search was proper.[110]

In *United States v. Cotterman*, a Ninth Circuit *en banc* panel held that there must be reasonable suspicion under the Fourth Amendment for a "forensic" search of a laptop at the border.[111] The court noted that forensic searches are much more intrusive, as they have the ability to unlock protected material and restore deleted content and viewed materials with sophisticated software.[112] However, the court also found that a manual search of an electronic device is "routine," and, therefore, warrantless and suspicionless searches of this kind do not violate the Fourth Amendment.[113] The court refused to accept an "anything goes" approach in favor of an approach that understands the importance of protecting privacy.[114] The Fourth Circuit later concurred and held that "a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion."[115]

However, more recently, a circuit split has arisen on the question of whether any particularized suspicion is needed to perform forensic searches.[116] Both *United States v. Kolsuz* and *United States v. Touset* were decided in 2018, yet the Fourth Circuit and Eleventh Circuit disagreed on whether individualized suspicion was required for a forensic search of electronic devices.[117] The Fourth Circuit in *Kolsuz*, relying on *Riley v. California*[118] and the sensitivity of the information on an electronic device, found the search too intrusive to be treated as routine.[119] The Eleventh Circuit in *Touset*, on the other hand, distinguished x-rays and strip searches as much more intrusive compared to a search of property, such as an

109. *Id.*
110. *Id.* at 1010.
111. United States v. Cotterman, 709 F.3d 952, 966–68 (9th Cir. 2013).
112. *Id.*
113. *Id.*
114. *Id.* (citation omitted).
115. United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018).
116. *Compare id.* at 137 (deciding that, especially in light of *Riley* and the invasiveness of a search of a digital phone, there must be individualized suspicion to perform a forensic search), *with* United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) (holding that because a forensic search of an electronic device is not as intrusive as a strip search or x-ray, even though it is intrusive, it is just a search of property and no suspicion is required).
117. *Kolsuz*, 890 F.3d at 137; *Touset*, 890 F.3d at 1234.
118. *Kolsuz*, 890 F.3d at 144–46.
119. *Id.*

electronic device, and found that such a search was routine.[120] While the 2018 Directive does distinguish between an advanced and basic search, it is still unclear whether suspicion is constitutionally mandated for an advanced search and if the Supreme Court will take up either of these cases.

C. RECENT ISSUE OF ELECTRONIC DEVICES AND THE BORDER SEARCH EXCEPTION

The border search exception's extension to electronic devices has prompted various points of contention. For instance, how far should a search go when it comes to an electronic device? In his argument to the Fourth Circuit, Ickes pointed out that a decision to extend the border search exception doctrine would be "sweeping," predicting that any persons travelling with a laptop would be subjected to a search of the laptop's contents.[121] The Fourth Circuit rejected this as "far-fetched" because the CBP does not have "the time nor the resources to search the contents of every computer."[122] This argument by the Fourth Circuit given in 2005 is less convincing because these types of searches are now relatively automatic and easy to do. Even supposing this had been true at the time, President Trump has been attempting to throw a lot of resources in the CBP's direction. More importantly, the CBP has been interested in doing these searches at an accelerated rate.[123] As previously discussed, even if this decision has not led to every computer passing through the border being searched as was Ickes' prediction, there has been a steep increase since 2005. Further, technological advancements have allowed quicker and deeper searches of electronic devices.[124] Furthermore, devices also hold much more data than they did when these searches began. In 2018, an iPhone X can hold 512 GB of data,[125] but in 2005 (when the Fourth Circuit decided *Ickes*) an iPhone did not even exist.[126] Technology is rapidly growing and a device in the palm of your

120. *Touset*, 890 F.3d at 1234.

121. United States v. Ickes, 393 F.3d 501, 506–07 (4th Cir. 2005).

122. *Id.* at 507.

123. On January 5, 2018, the CBP released updated statistics on border searches of electronic devices. Press Release, U.S. Customs & Border Prot., *supra* note 16. In 2017, 30,200 devices were searched compared to 19,051 in 2016. *Id.* This means that 0.007% of internationally arriving travelers had their devices searched in 2017, compared to 0.005% in 2016. *Id.*

124. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 864–67 (2004) (discussing the effect of technological advances on Fourth Amendment searches).

125. *IPhone Xs Tech Specs*, APPLE, https://www.apple.com/iphone-xs/specs (last visited Aug. 25, 2019).

126. Press Release, Apple, Inc., Apple Reinvents the Phone with iPhone (Jan. 9, 2007), https://www.apple.com/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone.

hand can hold exceedingly more information.

Should sensitive data be subject to a search? As reported by Vice, in 2017, a woman was denied entry to the United States when the CBP uncovered email correspondence on her phone with a doctor relating to her illegal substance overdose.[127] Various confidential and privileged information is found on our devices, and the Fourth Amendment does not seem to protect that information from being read by officers.

Additionally, in the pivotal 2014 Supreme Court decision *Riley v. California*, the Court declined to extend the search incident arrest doctrine to phones.[128] Police must now secure a warrant to search a phone, and cannot conduct warrantless searches just because the phone is on the body of the person arrested.[129] The Court specifically pointed out that cellphones are different from other items that can be found on a person during an arrest.[130] In today's world, people keep every piece of information on these devices, "from the mundane to the intimate."[131] The question now becomes whether *Riley*'s principle of treating electronic devices differently should be extended to border searches with respect to the Fourth Amendment.

Lastly, the 2018 Directive, although partially adopting *Cotterman*'s requirement of reasonable suspicion for forensic searches as CBP policy, still leaves many issues unresolved.[132] CBP officers do not need to have reasonable suspicion to conduct an advanced search when there is a "national security concern."[133] However, there is no definition or guidance for what a "national security concern" is, and it can be interpreted very broadly.[134] Second, even a basic search of an electronic device should not fall within the border search exception doctrine but instead should require reasonable suspicion or a warrant.

127. Allison Tierney, *Woman Banned from US After Border Agent Finds Proof of Drug Use on Phone*, VICE (Aug. 15, 2017, 2:15 PM), https://www.vice.com/en_us/article/ywwvxm/woman-banned-from-us-after-border-agent-finds-proof-of-drug-use-on-phone.

128. Riley v. California, 573 U.S. 373, 384–87 (2014).

129. *Id.*

130. *Id.* at 393–97.

131. *Id.* at 395 (citation omitted).

132. Sophia Cope & Aaron Mackey, *New CBP Border Device Search Policy Still Permits Unconstitutional Searches*, ELECTRONIC FRONTIER FOUND. (Jan. 8, 2018), https://www.eff.org/deeplinks/2018/01/new-cbp-border-device-search-policy-still-permits-unconstitutional-searches.

133. U.S. CUSTOMS & BORDER PROT., 2018 DIRECTIVE, *supra* note 19, at 5.

134. *See* Cope & Mackey, *supra* note 132.

III. THE FIFTH AMENDMENT: BALANCING SELF-INCRIMINATION AND PROTECTING YOUR DEVICE

A. BACKGROUND ON THE FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION

The Fifth Amendment protects individuals from "be[ing] compelled in any criminal case to be a witness against himself [or herself] . . . ."[135] Historically, this clause has been interpreted to cover any testimonial activity.[136] In order to invoke the Fifth Amendment's privilege against self-incrimination, a person must show: "(1) compulsion, (2) a testimonial communication or act, and (3) incrimination."[137] Moreover, the Fifth Amendment protection from self-incrimination applies not only in the courtroom but also during any official interrogation.[138]

Testimonial activity, the second requirement, has been broadly interpreted to even include any documented communication.[139] However, blood samples, handwriting samples, and voice exemplars have not been considered "testimonial" activities.[140] Today, as electronic devices have garnered greater prominence in our society and have proved instrumental in criminal investigations, a myriad of issues around accessibility and protections provided for by the Fifth Amendment have surfaced.

Further, an individual must also show that the act or communication being compelled would be incriminating, meeting the third requirement. With respect to CBP searches at the border, it would require a traveler to claim there is something incriminating on his or her device in order to invoke a Fifth Amendment right not to unlock the device, which is a difficult condition to meet. This presents at least two important issues. First, given the vast amount of information on a device, a person may be unaware of potential illegal documents on his or her phone. Individuals unknowingly download pirated information, or have perhaps a device that has contracted a virus that is importing illegal activity.[141] Second, if a person does know of

135. U.S. CONST. amend. V.

136. *See, e.g.*, Miranda v. Arizona, 384 U.S. 436, 461 (1966).

137. *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1341 (11th Cir. 2012) (citation omitted).

138. *Miranda*, 384 U.S. at 461.

139. Fisher v. United States, 425 U.S. 391, 408 (1976) ("The pronouncement . . . that a person may not be forced to produce his private papers has . . . often appeared as dictum in later opinions of this Court.").

140. New York v. Quarles, 467 U.S. 649, 666–67, 671 (1984) (O'Connor, J., concurring in part and dissenting in part).

141. However, the Fifth Amendment does cover compelled "information that may 'lead to

any criminal behavior on his or her device, it is somewhat self-incriminating in itself to inform officers there may be reason to conduct a more invasive search on the devices.

Consistently, the Fifth Amendment privilege against self-incrimination has been upheld and expanded beyond the black and white interpretation of the amendment's text.[142] The Supreme Court itself has exclaimed that it has "been zealous to safeguard the values that underlie the privilege,"[143] which "reflects many of our fundamental values and most noble aspirations . . . ."[144] It is still unclear, however, whether the privilege prevents officers from asking and compelling travelers to unlock devices on the border, regardless of the method of protection used on the device.

B. PASSWORDS, ENCRYPTIONS, AND THE FIFTH AMENDMENT PRIVILEGE

According to a 2017 study, 72% of smartphone owners use some sort of lock or encryption to protect their devices.[145] People store important personal information (for example, bank accounts, private documents, and so forth) and conduct business (for example, paying bills, purchasing items, and so forth) on their devices so commonly that they find a need to make some attempt to protect their devices from intrusion.[146]

Given that a plethora of information is contained on a cellphone, the reasons that law enforcement sees the value in looking through devices to augment its case or investigation are self-explanatory. Hence, the government has attempted to compel individuals to hand over any such password enabling the government to easily search a device. While no case has been decided by the Supreme Court on the issue of passwords, lower courts have leaned towards protecting passwords and encryptions under the

incriminating evidence' . . . even if the information itself is not inculpatory." United States v. Hubbell, 530 U.S. 27, 38 (2000) (quoting Doe v. United States, 487 U.S. 201, 208 n.6 (1988)).

142. The Fifth Amendment has been judicially expanded to apply to civil trials, criminal trials, grand jury proceedings, congressional investigations, juvenile proceedings, pretrial interrogations, and as a prophylactic against illegally obtained evidence in certain circumstances. Geoffrey B. Fehling, Verdugo*, Where'd You Go?:* Stoot v. City of Everett *and Evaluating Fifth Amendment Self-Incrimination Civil Liability Violations*, 18 GEO. MASON L. REV. 481, 490 (2011).

143. Kastigar v. United States, 406 U.S. 441, 445 (1972).

144. Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964).

145. Monica Anderson, *Many Smartphone Owners Don't Take Steps to Secure Their Devices*, PEW RES. CTR. (Mar. 15, 2017), https://www.pewresearch.org/fact-tank/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices.

146. *See* Roberto Baldwin, *Don't Be Silly. Lock Down and Encrypt Your Smartphone*, WIRED (Oct. 26, 2013, 6:30 AM), https://www.wired.com/2013/10/keep-your-smartphone-locked.

Fifth Amendment.[147]

1. Legal Foundation

While the issue of password-protected devices has yet to be decided by the Supreme Court, a legal foundation has been put in place to determine what meets the standard of "testimonial." Whether passwords are testimonial controls whether an individual can invoke the Fifth Amendment to prevent compulsion of the password.

United States v. Fisher established the reach of the Fifth Amendment to a situation where an individual is compelled to produce incriminating evidence against him- or herself.[148] *Fisher* dealt with a taxpayer being investigated by the Internal Revenue Service ("IRS") for federal income tax violations.[149] The IRS, learning of certain documents sent to the taxpayer's attorneys, summoned the production of these documents.[150] The Court held that because the "existence and location of the papers [were] a foregone conclusion" there was no self-incrimination in forcing the handing over of such documents and the Fifth Amendment was not implicated.[151] The location and contents of such papers were firmly known to the government, and therefore the taxpayer's compelled information "add[ed] little or nothing to the sum total of the Government's information . . . ."[152] Therefore, the government did not impede on the taxpayer's Fifth Amendment rights.[153] Thus, the "foregone conclusion" doctrine was born, which plays a vital role in determining violations of the Fifth Amendment right against self-incrimination.[154]

Additionally, in a string of cases the Supreme Court tried to determine what acts of compulsion actually constitute a violation of the Fifth Amendment. For example, in 1988, the Supreme Court was faced with whether a compelled act constitutes testimony.[155] In *Doe v. United States*, an individual under investigation for criminal acts was compelled to provide access to foreign bank records.[156] In this case, the Supreme Court determined

147. *E.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010).
148. Fisher v. United States, 425 U.S. 391, 411 (1976).
149. *Id.* at 394.
150. *Id.* at 394–95.
151. *Id.* at 411.
152. *Id.*
153. *Id.*
154. *See id.*
155. Doe v. United States, 487 U.S. 201, 202–04 (1988).
156. *Id.* at 203.

that it was not a violation of his Fifth Amendment because he did not admit or testify to anything incriminating.[157] However, in *United States v. Hubbell*, the Supreme Court determined that if an individual is required "to make extensive use of 'the contents of his own mind'" then he or she has the right to refuse under the Fifth Amendment.[158] After *Hubbell*, "the contents of one's mind" standard has made it unclear whether there is a cognitive requirement for invoking the Fifth Amendment right against self-incrimination.[159]

Lower courts have grappled with how to apply this precedent to encryptions and passwords. While courts have come up with alternative tests and applications of precedent, at least one lower court has found that the Fifth Amendment protects the compelling of one's electronic passwords.[160] For example, in *United Sates v. Kirschner*, the government compelled the disclosure of passwords associated with a computer in an effort to secure evidence supporting a child pornography allegation.[161] The alleged child pornographer refused to hand over his passwords, asserting his Fifth Amendment privilege against self-incrimination.[162] The court held that such compulsion of a password violated the Fifth Amendment as "the government [was] not seeking documents or objects—it [was] seeking testimony from the Defendant, requiring him to divulge through his mental processes his password—that will be used to incriminate him."[163] Here, the court distinguished *Kirschner* from *Doe*: in *Kirschner* the compelled passwords would convey incriminating knowledge (the password) to the government, whereas in *Doe*, the password would only give the government access to information.[164] Various other state and district courts have agreed, either through decisions or dictum, that the compulsion of a password or encryption key amounts to testimonial action protected by the Fifth Amendment right against self-incrimination.[165]

157. *Id.* at 219.

158. United States v. Hubbell, 530 U.S. 27, 43 (2000) (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)).

159. *See* Chase Bales, Note, *Unbreakable: The Fifth Amendment and Computer Passwords*, 44 ARIZ. ST. L.J. 1293, 1299–300 (2012).

160. United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010).

161. *Id.* at 666.

162. *Id.*

163. *Id.* at 669.

164. *Id.*

165. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1341–52 (11th Cir. 2012); United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982, at *54 (N.D.N.Y. May 24, 2006); Commonwealth v. Gelfgatt, 11 N.E.3d 605, 612 (Mass. 2014).

2. Electronic Searches at the Border and the Fifth Amendment Today

The issue concerning compelling passwords and the Fifth Amendment at the border has already begun to present itself in courtrooms. In 2006, while crossing the Derby Line Port of Entry, CBP officers conducted a search of Sebastien Boucher's car and found a laptop computer.[166] The names of particular files on the computer led officers to suspect that they contained child pornography or other evidence of criminal behavior.[167] The officers attempted to conduct a forensic search on Boucher's laptop but failed because the device was password-protected.[168] A grand jury then issued a subpoena for passwords protecting any information on the laptop computer seized at the border, but Boucher argued that being forced to provide his passwords violated his Fifth Amendment right against self-incrimination.[169] Although a magistrate judge quashed the subpoena on Fifth Amendment grounds,[170] the district court found that the information was a "foregone conclusion" because the government needs only to know what and where the files were with "reasonable particularity."[171] Even though the district court overruled the magistrate judge's decision, the court did not negatively comment on the magistrate judge's reasoning that, by having Boucher type the password himself, he would be divulging that he has control over the device, which is, in itself, incriminating.[172]

In 2012, the Eleventh Circuit held that the Fifth Amendment privilege protected a person's encrypted hard drive when he was also accused of possessing child pornography.[173] The court found that revealing one's password would amount to "testimonial" activity and was protected by the Fifth Amendment because the decryption of the hard drive "would require the use of the contents of [his] mind and could not be fairly characterized as

166. *In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *4 (D. Vt. Feb. 19, 2009).

167. *Id.*

168. *Id.* at *5.

169. *Id.* at *2.

170. *In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2007 U.S. Dist. LEXIS 87951, at *9 (D. Vt. Nov. 29, 2007), *rev'd*, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009).

171. *Boucher*, 2009 U.S. Dist. LEXIS 13006, at *8 (quoting, respectively, Fisher v. United States, 425 U.S. 391, 411 (1975) and *In re* Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993)).

172. *Id.* at *6–11; Andrew T. Winkler, *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technological Era*, 39 RUTGERS COMPUTER & TECH. L.J. 194, 201 (2013).

173. *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1352 (11th Cir. 2012).

a physical act that would be nontestimonial in nature."[174] However, the court also found that this Fifth Amendment protection did not apply if the testimonial statements were a "foregone conclusion" in that the government knew the "location, existence, and authenticity of the purported evidence . . . with reasonable particularity . . . ."[175]

Additionally, in *United States v. Fricosu*, a district court found that, because a name on the computer indicated ownership, and because the person likely had incriminating files, the foregone conclusion doctrine also applied and barred a Fifth Amendment argument against compelling the defendant to provide her password.[176]

However, because the Supreme Court has yet to resolve the divergent approaches to whether the Fifth Amendment privilege protects against providing passwords to devices that contain incriminating evidence, it is unclear whether one can invoke this same privileged at the border and refuse to hand over a password. Even so, it is unclear whether travelers would know they have this option, and even if they do, whether invoking the privilege is worth delaying their passage.

C. BIOMETRIC AUTHORIZATION

While the Fifth Amendment may protect individuals from having to hand over their passwords at the border absent the foregone conclusion exception applying, the same may not also be said for phones that can be unlocked with a fingerprint or other forms of biometric authorization.[177] Biometrics, the practice of using one's distinctive traits for detection by an electronic device,[178] is becoming a widely popular way to safeguard personal devices.[179] Hackers have become more sophisticated, and the breaches of companies such as Equifax have prompted many to look for more secure

174. *Id.* at 1346.

175. *Id.* at 1344.

176. United States v. Fricosu, 841 F. Supp. 2d 1232, 1237–38 (D. Colo. 2012). In *Fricosu*, the government knew the location and existence of the documents on the computer. The fact that it did not know the specific content of the documents did not matter. All the government needed to show, in addition, was that, by a preponderance of evidence, the computer belonged to the defendant and that she was the sole or primary user. *Id.*

177. Jack Linshi, *Why the Constitution Can Protect Passwords But Not Fingerprint Scans*, TIME (Nov. 6, 2014), http://time.com/3558936/fingerprint-password-fifth-amendment.

178. *See generally* RAWLSON O'NEIL KING, BIOMETRICS RESEARCH GRP., BIOMETRICS AND BORDER SECURITY (2016), http://www.biometricupdate.com/201606/special-report-biometrics-and-border-security.

179. Steven Norton, *What Comes After Passwords?*, WALL ST. J. (Sept. 17, 2017, 10:04 PM), https://www.wsj.com/articles/what-comes-after-passwords-1505700241.

ways to ensure the security of their data.[180]

Since Apple introduced "Touch ID" in 2013, fingerprint authorization has become more mainstream.[181] With Apple's Touch ID, the chances of another person's finger having the ability to unlock a device is one in 50,000,[182] prompting many to believe their phone or device is more secure than with a generic four-digit passcode. However, courts do not treat a fingerprint the same as they do a traditional password.[183]

Some argue fingerprints are not testimonial in the way passwords are, given that passwords are held in your mind, while fingerprints are physical attributes.[184] Recently, in a Minnesota appeals case, a man accused of robbery was compelled to provide his fingerprint to unlock his cellphone.[185] The court held that the defendant's Fifth Amendment rights were not violated because "compelling [the defendant] to produce his fingerprint to unlock the cellphone did not require a testimonial communication . . . ."[186] Similarly, in a Virginia case against a man who used his smartphone to videotape an alleged assault, the court held that a defendant could be compelled to produce his fingerprint to unlock his phone, and that this was not in violation of his Fifth Amendment rights.[187] The court argued that a fingerprint did not require him to "communicate any knowledge" nor did it require him to "disclose contents of his own mind" like a password would.[188]

Smartphone and electronic device creators, perhaps realizing this issue, have created new safeguards. For instance, in the recently upgraded iPhones, a traditional password is required for unlocking a phone once it has been

180. *Id.*

181. Press Release, Apple, Inc., Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World (Sept. 10, 2013), https://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World; J.V. Chamary, *No, Apple's Face ID Is Not a 'Secure Password'*, FORBES (Sept. 18, 2017, 11:00 AM), https://www.forbes.com/sites/jvchamary/2017/09/18/security-apple-face-id-iphone-x/#7bd854664c83.

182. Andrea Chang & Samantha Masunaga, *Apple Says iPhone X's Face ID Can't Be Easily Spoofed. But Your Face Isn't Exactly Private*, L.A. TIMES (Sept. 12, 2017, 7:00 PM), http://www.latimes.com/business/technology/la-fi-tn-apple-iphone-face-id-20170913-story.html.

183. Matthew J. Weber, Note, *Warning—Weak Password: The Courts' Indecipherable Approach to Encryption and the Fifth Amendment*, 2016 U. ILL. J.L. TECH. & POL'Y 455, 471.

184. Thomas Brewster, *Federal Court: Cops Can't Just Walk into a Building and Force Unlock iPhones with Fingerprints*, FORBES (Feb. 22, 2017, 3:41 PM), https://www.forbes.com/sites/thomasbrewster/2017/02/22/federal-court-cops-cants-just-walk-into-a-building-and-force-unlock-iphones-inside/#6994403f3412.

185. State v. Diamond, 890 N.W.2d 143, 145–46 (Minn. Ct. App. 2017).

186. *Id.* at 151.

187. Commonwealth v. Baust, 89 Va. Cir. 267, 271 (2014).

188. *Id.*

turned off or once it has been unused for over forty-eight hours.[189] It is unclear how the courts will address whether a person should be required to unlock his or her phone in other ways if a fingerprint could have been used.[190]

Facial recognition, another biometric security function, is gaining attention, especially with its relation to the new iPhone X and future iPhone generations.[191] Facial recognition adds another layer of complication when you take into account that a specific facial expression may be needed to unlock a device.[192] The current iPhone "Face ID" supposedly requires nothing but the phone pointed at your face, making it very much similar to Touch ID.[193] However, if a certain face is needed for some technology, the question then becomes how to determine the line between testimonial (and in your mind) authorization and physical authorization, especially if the facial expression is something uniquely correlated with unlocking your device.[194]

A variety of prominent companies are following suit in the biometric identification trend, including MasterCard who is testing heartbeat data and Google who is testing speech patterns.[195] Soon facial recognition and fingerprint identification will no longer be the newest technologies to ensure security of a personal electronic device. With these new technologies, the line between what is testimonial, and therefore protected under the Fifth Amendment, and what is not will become harder to define.

189. Glen Kopp & Kedar Bhatia, *Fingerprint Lock Won't Protect Phone from Law Enforcement*, LAW360 (Dec. 12, 2014, 9:55 AM), https://www.law360.com/articles/603831/fingerprint-lock-won-t-protect-phone-from-law-enforcement.

190. *Id.* New Apple technology also requires a passcode if there are more than five failed Touch ID attempts. People can cheat the system and use the wrong finger or hold it the wrong way if it means that officers will no longer have access to the phone without a password that only he or she knows, which is protected by the Fifth Amendment. *See* Ben Lovejoy, *Suspect Required to Unlock iPhone Using Touch ID in Second Federal Case*, 9TO5MAC (Jul. 25, 2016, 7:33 AM), https://9to5mac.com/2016/07/25/touch-id-fingerprint-fbi-law.

191. Apple is touting this new technology as a better way to protect your phone because the chance another person could unlock an iPhone with a fingerprint was one in 50,000, but now the chance with Face ID is one in a million. *See* Chang & Masunaga, *supra* note 182.

192. Adi Robertson, *Why Face ID Won't Give You the Legal Protection of a Passcode*, THE VERGE (Sept. 12, 2017, 6:54 PM), https://www.theverge.com/2017/9/12/16298192/apple-iphone-face-id-legal-security-fifth-amendment.

193. Press Release, Apple, Inc., The Future Is Here: iPhone X (Sept. 12, 2017), https://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x.

194. *Id.*

195. Haydn Evans, *The State of Biometrics Technology: The Uses, the Concerns*, LAW360 (Aug 8, 2017, 12:20 PM), https://www.law360.com/articles/950365/the-state-of-biometrics-technology-the-uses-the-concerns.

D. COMPELLING BIOMETRIC AUTHORIZATION SHOULD BE TREATED AS COMPELLING PASSWORDS AT THE BORDER

There is something disturbing about the notion that the same information secured by a fingerprint or facial recognition is less secure from the government at the border than a traditional password when people have been led to believe this is the most protected manner to secure one's device. Justice Stevens said in his dissent in *Doe v. United States* that while "in some cases [a person may] be forced to surrender a key to a strongbox containing incriminating documents," Justice Stevens did "not believe [a person could] be compelled to reveal the combination to his [or her] wall safe—by word or deed."[196] With this in mind, the Fifth Amendment's purpose has been interpreted broadly with regard to preventing people from being compelled to incriminate themselves.[197] The Founding Fathers could not have foreseen the invention of technology nor its evolution to this scale, but the idea that one should not have to incriminate oneself should stand firm. The Founding Fathers would have only thought of keys that opened physical spaces to physical things.

Although compelling a fingerprint does not require communication, it can require action on the part of the person and is similar to a number or letter password in that it is something of yours that unlocks a device; therefore, compelling biometric authorization should not be allowed under Fifth Amendment principles in the same way a traditional password is protected. For instance, various courts have noted that inputting a password is an act that in itself could be incriminating and against Fifth Amendment protections merely because it conveys control over the device.[198] Similarly, putting your face in front of a phone or finger on a device is an "act" that is all that is needed to meet the Fifth Amendment's standard. Additionally, the argument that an officer can just hold your phone to your finger or your face, without action on an individual's part, is not convincing because it is akin to compelling speech—the government is compelling authorization.

In *Pennsylvania v. Muniz*, the Court suggested that Fifth Amendment protections could even be expanded to written statements.[199] The Court explained that testimonial communications "written, oral or otherwise" that reveal "consciousness" of fact warrant Fifth Amendment protection because

196. Doe v. United States, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting).
197. *See, e.g.*, Miranda v. Arizona, 384 U.S. 436, 467 (1966).
198. *See, e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 668 (2010).
199. Pennsylvania v. Muniz, 496 U.S. 582, 598 (1990).

they divulge the "the contents of [one's] own mind,"[200] This—biometric authorization—is the "otherwise." The government is compelling communication of one's physical attributes to the device, which simply goes against the Fifth Amendment right against self-incrimination. Unlike other physical evidence, such as blood samples and handwriting exemplars, passwords give the government access to information with use of one's body or mind.

Given that biometric authorization compels an individual to incriminate him- or herself, it should not be part of the CBP policies at the border. As discussed above, the Court has been respectful of the policies behind the Fifth Amendment privilege including the "sense of fair play" and the "right of each individual 'to a private enclave where he may lead a private life' . . . ."[201] Today, phones hold all of one's private information and compelling one to open that window hardly feels fair.

E. THE FIFTH AMENDMENT PRIVILEGE SHOULD APPLY TO THE COMPULSION OF BOTH PASSWORDS AND BIOMETRIC AUTHORIZATION AT THE BORDER

CBP and ICE officers should no longer be able to compel travelers to unlock their devices, regardless of what authorizing or securing function is protecting the devices. The Fifth Amendment Right against self-incrimination has a long and respected past that forbids the compulsion of such information during official interrogations.[202] While CBP officers are detaining travelers for questioning, the travelers should still have the rights they would normally have in any other official interrogation anywhere else. The Supreme Court in *Hubbell* importantly claimed that the Fifth Amendment protects individuals from being compelled to reveal "the contents of his [or her] own mind . . . ."[203] Passwords should thus be protected if the password is only known to the traveler in his or her mind and is akin to compelling someone to reveal direct information that could incriminate him or herself—something the Fifth Amendment firmly stands against.

200. *Id.* at 594 (quoting Doe v. United States, 487 U.S. 201, 210–11 (1988)).

201. Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964) (quoting United States v. Grunewald, 233 F.2d 556, 581–82 (2d Cir. 1956) (Frank, J., dissenting)).

202. *See, e.g.*, Miranda v. Arizona, 384 U.S. 436, 461 (1966) ("[T]he compulsion to speak in the isolated setting of the police station may well be greater than in courts or other official investigations, where there are often impartial observers to guard against intimidation or trickery.").

203. United States v. Hubbell, 530 U.S. 27, 43 (2000) (citing Curcio v. United States, 354 U.S. 118, 128 (1957) and Doe v. United States, 487 U.S. 201, 210 (1998)).

Furthermore, biometric authorization should be protected by the Fifth Amendment the same way a traditional password does. First, if the Fifth Amendment protects passwords, it should protect all passwords—regardless of what technology is employed. It would be hardly consistent for a court to favor one sort of security measure over another. Second, biometric authorization holds the same principles as the ideas protected by the Fifth Amendment. For instance, a fingerprint is your own, something you have control over and can place with cognition on your device to unlock it. Your intention to unlock it follows similarly to you pressing your finger against the device in the same way you intend to unlock your computer by typing in a few letters. Lastly, the principle behind the Fifth Amendment's protection against self-incrimination is that no person should be compelled to incriminate themselves. That is exactly what the CBP and ICE are doing. They are compelling travelers to unlock devices in order to let the government find evidence. This would not stand in the outside world. A warrant or probable cause is strictly upheld and respected. There is no reason why, by simply crossing into the United States, an individual would not have this protection. There is nothing in history nor the border search exception that supports piercing the Fifth Amendment or making any such exception to its protections.

Even if courts decide that biometric authorization is not protected under the Fifth Amendment right against self-incrimination, perhaps other steps can be taken to protect devices at the border from this infringement. For instance, similar to how Apple has created a need for password authentication for recently unused or turned off devices, Apple devices can require a password when in the vicinity of an international airport. Further, educating individuals, especially those with sensitive materials, such as attorneys and doctors, to lock their devices only with traditional passwords can prevent such abuses by the CBP to sidestep the Fifth Amendment because there is another unlocking mechanism. The CBP's practices of intimidation, such as saying it will detain devices, is only empowered by the fact that the CBP itself is not intimidated by the Fifth Amendment's authority in these situations. By making the Fifth Amendment's protection of passwords and biometric authorization more pronounced and clearer in courts and CBP directives, travelers will no longer be wrongly compelled to incriminate themselves.

IV. THE FIRST AMENDMENT SHOULD PROTECT YOUR DEVICE FROM BEING SEARCHED AT ALL WITHOUT A WARRANT OR REASONABLE SUSPICION

A. INTERPRETING THE FIRST AMENDMENT TO COVER ANONYMITY

Regardless of whether the Fifth Amendment protects travelers from being compelled to unlock their devices, the First Amendment should protect personal electronic devices from government searches at the border. The First Amendment states in part that Congress should not "abridg[e] the freedom of speech . . . ."[204] The First Amendment, however, much like the Fifth, has been interpreted beyond a bare reading of its text to encompass anonymity in speaking, reading, obtaining, exchanging, and associating with any such free speech.

1. Anonymous Speech

Since the Founding, the First Amendment has purportedly protected anonymous speech;[205] undoubtedly, this is because anonymous speech importantly promotes and gives way to open and frank discussion. In fact, some Founding Fathers even employed the benefits of anonymous speech themselves when writing the Federalist Papers under the anonymous pseudonym "Publius."[206] The Supreme Court, acknowledging the significance of protecting anonymity, has continually upheld a right to anonymous speech under the First Amendment, albeit with some exceptions. Specifically, the Court has pointed out that "an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression,"[207] and "[a]nonymity is a shield from the tyranny of the majority."[208]

The current foundation for the right to anonymous speech protected by the First Amendment stems from two seminal cases—*Talley v. California* and *McIntyre v. Ohio Elections Committee*.[209] In these cases, the Supreme Court found that the right to anonymous speech is supported by two points:

204. U.S. CONST. amend. I.

205. Jason M. Shepard & Genelle Belmas, *Anonymity, Disclosure and First Amendment Balancing in the Internet Era: Developments in Libel, Copyright, and Election Speech*, 15 YALE J.L. & TECH. 92, 94 (2012).

206. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 360 (1995) (Thomas, J., concurring in the judgment).

207. Talley v. California, 362 U.S. 60, 64 (1960).

208. *McIntyre*, 514 U.S. at 357 (citing J.S. MILL, ON LIBERTY, AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT 1, 3–4 (R.B. McCallum ed., 1947)).

209. *See id.* at 342; *Talley*, 362 U.S. at 60–66.

(1) the significant historical importance of anonymous speech in our political society and its growth, and (2) the concern that a threat of unveiling identities may stop the free flow of information and thoughts.[210] The Supreme Court has recently affirmed this right to anonymous speech in both the 1999 case of *Buckley v. American Constitutional Law Foundation* and in the 2002 case of *Watchtower Bible & Tract Society v. Village of Stratton*.[211]

However, currently, the internet has caused new concerns as anonymous speech can be more easily conducted and more widely spread than ever before.[212] Some of the speech can be quite damaging or dangerous, and lower courts have wrestled with how to weigh First Amendment rights against other rights and priorities.[213] For example, in defamation cases, courts have come up with a myriad of different frameworks to address these new questions, including the following: "the 'good faith' test; the . . . 'motion to dismiss' standard;" and the "state discovery and civil procedure rule application test[] . . . ."[214]

2. The Right to Read or Receive Information Anonymously

The First Amendment has also been repeatedly extended to the right to read or receive information.[215] The First Amendment does not only shield the political speaker at a rally but also the people in the audience and those listening to a recording of the speech in the privacy of their own homes.[216] They are two sides to the same coin—the giving and receiving of information—both protected by the First Amendment.

Although the right to read or receive information is firmly protected by the First Amendment, the right to do so anonymously is less confidently

210. *McIntyre*, 514 U.S. at 341–43, 350–53; *Talley*, 362 U.S. at 60–66; Jocelyn Hanamirian, Note, *The Right to Remain Anonymous: Anonymous Speakers, Confidential Sources and the Public Good*, 35 COLUM. J.L. & ARTS 119, 127 (2011).

211. *See* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166–67 (2002); Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 199 (1999).

212. *E.g.*, Julie Zhou, Opinion, *Where Anonymity Breeds Contempt*, N.Y. TIMES (Nov. 29, 2010), https://www.nytimes.com/2010/11/30/opinion/30zhuo.html (discussing the effect of anonymity—which research shows increases unethical behavior—on internet use).

213. Robert G. Larson & Paul A. Godfread, *Bringing John Doe to Court: Procedural Issues in Unmasking Anonymous Internet Defendants*, 38 WM. MITCHELL L. REV. 328, 336–41 (2011) (discussing various tests developed by lower courts to unmask anonymous internet speakers).

214. Jason A. Martin & Anthony L. Fargo, *Anonymity as a Legal Right: Where and Why It Matters*, 16 N.C. J.L. & TECH. 311, 340 (2015).

215. *See, e.g.*, Stanley v. Georgia, 394 U.S. 557, 565 (1969).

216. Marc Jonathan Blitz, *Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right to Read, and a First Amendment Theory for an Unaccompanied Right to Receive Information*, 74 UMKC L. REV. 799, 800 (2006).

assured. The foundation for the right to anonymous reading can be traced back to the McCarthy era and cases involving the government's inquiries into suspected communists.[217] During this time, the Supreme Court held that the government could not request the contents of a university lecture,[218] nor could legislative investigations be authorized to "probe the reading habits" of any persons.[219]

The right to read anonymously, however, is most directly supported by *Lamont v. Postmaster General*.[220] In *Lamont*, the Supreme Court struck down a statute that allowed the post office to refuse to deliver foreign-sent mail that contained communist propaganda.[221] The statute required addressees to send official requests for detained mail to be delivered, but the fear of letting the government know the addressees were reading information it believed to be potential communist propaganda deterred many from requesting deliveries.[222] The Supreme Court held that this practice infringed upon the recipients' First Amendment rights and was "at war with the 'uninhibited, robust, and wide-open' debate and discussion that are contemplated by the First Amendment" as people had the right to receive their mail anonymously so as not to be under the threat of communist suspicion.[223]

Further, the Court has held the right to receive information should be protected when there are other alternatives available that would be less restrictive. In *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, the Supreme Court struck down a statute requiring written requests be given for access to stations thought to be unsuitable for minors because there were less restrictive alternatives and the statute was more extensive than necessary to meet the need to protect minors.[224] Similarly, the Third Circuit struck down a statute imposing a requirement of identification in phone sex services because there was a less restrictive alternative.[225] The Third Circuit used a balancing test and held that, in this case, the government even had the burden to show that there was not a less restrictive way to serve

217. Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1007–08 (1996).

218. Sweezy v. New Hampshire, 354 U.S. 234, 250–51 (1957) (plurality opinion).

219. Schneider v. Smith, 390 U.S. 17, 24 (1968).

220. Lamont v. Postmaster Gen., 381 U.S. 301, 302–07 (1965).

221. *Id.*

222. *Id.* at 307.

223. *Id.* (quoting N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)).

224. Denver Area Educ. Telcomms. Consortium, Inc. v. FCC, 518 U.S. 727, 733 (1996).

225. Fabulous Assocs., Inc. v. Pa. Pub. Util. Comm'n, 896 F.2d 780, 787–88 (3d Cir. 1990).

the state's interest.[226]

Therefore, although the right to receive information anonymously has not been directly provided by the Supreme Court, it follows that the right to receive information quietly, without announcement, has been protected when weighed with the state's interest, especially when there are less restrictive means to meeting the state's objective. Importantly, it is also the government's burden to show that the result intended cannot be reached by any less speech-restrictive means.

3. Right to Associate Anonymously

Furthermore, although the First Amendment does not explicitly state that a person has a right to associate anonymously, the Supreme Court found in *NAACP v. Alabama* that the right to anonymously associate is in fact constitutionally protected.[227] In *NAACP*, a court ordered the NAACP to hand over membership lists to the state of Alabama, but the NAACP refused, claiming it was unconstitutional to compel production of its membership lists.[228] In Justice Harlan's opinion siding with the NAACP he noted the importance of the "vital relationship between freedom to associate and privacy in one's associations."[229]

In other cases, the Supreme Court has been faced with a state actor attempting to gain information on membership of minority groups, albeit sometimes with good intentions.[230] When there was no compelling state interest to outweigh the negative impacts of disclosing the anonymous members, the members have a First Amendment right to stay anonymous.[231] The courts, in refusing to force disclosure of members, protect groups from being targets and make it safer and easier for them to join causes, share and receive ideas from others, and feel comradery.

226. *Id.*

227. NAACP v. Ala. *ex rel*. Patterson, 357 U.S. 449, 462 (1958).

228. *Id.* at 452–54.

229. *Id.* at 462.

230. For instance, in *Shelton v. Tucker*, the Supreme Court held that it was unconstitutional and a violation of the First Amendment to require teachers to list every tie they had to any association in the last five years. Shelton v. Tucker, 364 U.S. 479, 496 (1960). The Court noted the following:

> There can be no doubt of the right of a State to investigate the competence and fitness of those whom it hires to teach in its schools . . . . There is "no requirement in the Federal Constitution that a teacher's classroom conduct be the sole basis for determining his [or her] fitness. Fitness for teaching depends on a broad range of factors."

Id. at 485 (quoting Beilan v. Board of Education, 357 U.S. 399, 406 (1958)). These factors may include a teacher's associational ties. *Id.* However, the requirement that teachers disclose all associational ties was "completely unlimited" and required disclosure of associations that "could have no possible bearing upon the teacher's occupational competence or fitness." *Id.* at 488.

231. *Id.* at 490.

4. The Court's Approach to First Amendment Claims Concerning Searches at the Border

Whether or not the First Amendment protects against searches in general is unclear as the Supreme Court has held that the First Amendment is not violated merely because expressive material is uncovered during an unconstitutional search.[232] However, the principles behind the First Amendment and its history of protecting anonymous speech, reading, and association should cause concern over searches as they are conducted today.

Specifically with respect to the border, in the past courts have generally refused to create any First Amendment carve out to the border search exception.[233] For instance, in *Ickes*, the traveler argued that there should be a complete First Amendment carve out to the border search exception when a search of his laptop at the border revealed child pornography in its contents.[234] Ickes claimed that the border search exception could not be applied to search "expressive" materials in any form.[235] The Fourth Circuit, in rejecting Ickes' argument, held that the history of customs and border policies supports these searches regardless of First Amendment concerns, that a First Amendment carve out to the border search exception doctrine would cause "significant headaches for those forced to determine its scope," and that public policy prefers giving the CBP such broad authority.[236] In fact, the court pointed out that

> national security interests may require uncovering terrorist communications, which are inherently "expressive." [Whereas] following Ickes's logic would create a sanctuary at the border for all expressive material—even for terrorist plans . . . undermin[ing] the compelling reasons that lie at the very heart of the border search doctrine.[237]

Similarly, the Ninth Circuit sided with *Ickes* in *Arnold* when it refused to carve out a First Amendment exception because such a rule would (1) "protect terrorist communications which are inherently 'expressive'"; (2) create a difficult standard for CBP officers; and (3) go against Supreme Court precedent that favors analyzing government activity under the Fourth

232. Zurcher v. Stanford Daily, 436 U.S. 547, 563–68 (1978).

233. *See* United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005).

234. *Ickes*, 393 F.3d at 503. Ickes also argued the search was unconstitutional on Fourth Amendment grounds, but the court also rejected this argument.

235. *Id.* at 506.

236. *Id.* at 505–06.

237. *Id.* at 506.

Amendment when a First Amendment issue is also alleged.[238] Thus, circuit courts have found that the state interest prevails against First Amendment rights during border searches because a rule that excludes expressive material from being searched would be unworkable, the allowable scope of such a search would be difficult to pin down, and the state's interest in uncovering terrorist activity is compelling.

However, since these cases in the mid-2000s, the Court's landmark *Riley* decision suggests *Ickes* and *Arnold* may no longer be the right approach. In *Riley*, the Court considered whether officers could search the contents of an individual's cellphone incident to arrest under the Fourth Amendment's search incident to arrest exception.[239] The Court ultimately declined to extend this exception to cell phones; police officers are now required to obtain a warrant before searching the contents of a cell phone discovered incident to arrest.[240] In doing so, the Court distinguished electronic phones from other physical property subject to the exception.[241] It is likely *Riley* may influence various other Fourth Amendment doctrines and their relationship to electronic devices.

In fact, in 2018, a federal district court in Massachusetts denied a motion to dismiss a First Amendment claim against the Government pertaining to searches of electronic devices at the border.[242] The court noted specifically that, given the "particular concerns raised by digital devices like cell phones" similar to those contemplated in *Riley*, "and the limitless search authorizations in the CBP and ICE policies, Plaintiffs [had] plausibly alleged that the government's digital device search policies substantially burden[ed] travelers' First Amendment rights."[243] The court was not persuaded that *Ickes* still controls, given that *Riley*, which postdates *Ickes*, delineates between "expressive material" and "cell phones."[244] Here, the court seemed to say there is a difference in protecting all "expressive material" at the border and just electronic devices, relying on *Riley*. Furthermore, the court again insinuated that *Ickes* is no longer the proper rule, given that the court acknowledged that a requirement subjecting "any person carrying a laptop computer . . . on an international flight . . . to a search of the files on the[ir]

238. United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008).

239. Riley v. California, 573 U.S. 373, 386 (2014).

240. *Id.*

241. *Id.*

242. Alasaad v. Nielsen, No. 17-cv-11730-DJC, 2018 U.S. Dist. LEXIS 78783, at *2–3 (D. Mass. May 9, 2018).

243. *Id.* at *76.

244. *Id.* at *73.

computer hard drive" may seem "far-fetched," but "the recent increase in border device searches and the expanding storage and functioning capacities of electronic devices . . . suggest otherwise."[245]

While this is only a district court's denial of a motion to dismiss, it is indicative of the way other courts may start to view *Ickes* and *Arnold*, which are the leading cases with respect to the First Amendment and border searches of electronic devices, in light of *Riley*.

B. CURRENT SEARCHES OF ELECTRONIC DEVICES AT THE BORDER VIOLATE THE FIRST AMENDMENT

Searches of electronic devices reveal written materials—shared or not shared—in any private or public forum, a history of materials read by the user, information including which groups or persons of interest the device-owner "follows" or has a relationship with via the internet, and much more. This information all falls under the protections under the First Amendment—even though some courts have not found this to be a violation—and First Amendment rights should not be vitiated by the border search exception.

As previously discussed, the Supreme Court has consistently upheld the right of a person to speak anonymously.[246] Without this protection, those wishing to share unpopular opinions will refrain from doing so, while those who agree with popular opinion will not. The minority voice will be silenced with no change to the majority's, and, therefore, the exchange of ideas will be limited. The power of anonymity is pierced by the government when it searches devices at the border. For instance, when searching a device, officers have access to a variety of applications and web histories that can reveal blog or social media pseudonyms controlled by the device owner. Hypothetically, a traveler who has a Twitter account praising non-violent traditional Muslim values, which is harmless in itself and merely promotes a religious belief, may think again about posing such views if he knows that, at the border, the government can compel its production and scrutinize him for being Muslim. Would Thomas Paine have published *Common Sense* had he not been promised anonymity? Would the Constitution have been ratified without the anonymous Federalist Papers? Would Benjamin Franklin's works have been published had he not used a pen name?[247] Would various

245. *Id.* at *73–74 (first alteration in original) (quoting United States v. Ickes, 393 F.3d 501, 506–07 (4th Cir. 2005)).

246. *E.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Talley v. California, 362 U.S. 60, 64 (1960).

247. For a discussion of the value of anonymous criticism to U.S. history, including Paine's

female writers have had readers had they not used male names instead of their own?[248] Any such hesitation chills free speech, an impact justices have continually been wary of causing.[249] In this way, those owning anonymous accounts to speak out against the President, promote an unpopular faith, discuss abortion, and so forth—knowing that their anonymous accounts are susceptible to revelation at the border—may think again before posting or sharing any of these ideas.

While *Talley* and *McIntyre* still remain good law, the right to anonymous speech is far from absolute. As discussed above, with the growth of the internet and related platforms, there have been various devices put in place by the Court to weigh the interests of piercing anonymity against the dangers of not doing so. Here, the benefits of stopping a small number of criminals by using suspicionless searches of devices is outweighed by the consequences of diminishing free and open speech. It was not always the prerogative of the CBP to search emails, and we have other intelligence agencies who scan the internet for terrorist activity and communication.[250] The price of searching thousands of phones causing widespread self-censorship does not outweigh the added ease of catching a criminal by mere happenstance that he or she is at the border or international airport.

Further, electronic devices hold various amounts of information that can reveal the readings and associations of the user. The back-memories of these devices reveal the Internet pages that the user has viewed, the duration and frequency of these views, and whether a person "follows" a speaking person or group.[251] Much like *Lamont*, customs officers are acting like the post office scanning read materials, and this has the same effect of intimidating people from reading information protected by the First Amendment. Just as in *Lamont*, it should be unacceptable for the mere point

Common Sense, the Federalist Papers, and works by Benjamin Franklin, see Jordan E. Taylor, *Anonymous Criticism Helped Make America Great*, WASH. POST (Sept. 8, 2018), https://www.washingtonpost.com/outlook/2018/09/08/anonymous-criticism-helped-make-america-great/?noredirect=on.

248. Charlotte, Emily and Anne Brontë used the names Currer, Ellis, and Acton Bell; Mary Anne Evens used George Eliot; Louisa May Alcott used A.M. Barnard; and Nelle Harper Lee used plainly Harper Lee. Sara Semic, *Unmasking the Author Identities Behind the Aliases*, ELLE (Apr. 10, 2016), https://www.elle.com/uk/life-and-culture/culture/articles/a32148/author-aliases-unmasked.

249. *See, e.g.*, Lamont v. Postmaster Gen., 381 U.S. 301, 307 (1965) (referring to this effect as the "deterrent effect"); N.Y. Times Co. v. Sullivan, 376 U.S. 254, 291–92 (1964).

250. *See generally Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing before the S. Comm. on the Judiciary*, 114th Cong. (2015) (statement of Sally Wuillian Yeates, Deputy Att'y Gen., Department of Justice and James B. Comey, Director, Federal Bureau of Investigation) (discussing the federal government's technological capabilities with respect to digital privacy).

251. *See* Riley v. California, 573 U.S. 373, 396 (2014).

that it deters individuals from freely reading noncriminal information in fear of retaliation or misunderstanding.

Additionally, today, it is much easier to find out what someone may believe by seeing how he or she associates him or herself. With the advent of Facebook, Twitter and other social media sites, simple access to one's account can lead to discoveries into the user's political and religious views by seeing what groups he or she has friended, followed, liked, or shared.[252] The fear of unveiling this information may deter people from associating themselves in any online forum, against the promise of the First Amendment. This is especially important in today's world: people may be afraid to associate themselves with extremely polarizing groups—such as tea-party republicans, transgender rights advocacy groups, Anti-Trump campaigns, and many more—in fear of losing their jobs or being targeted for those beliefs. Some may have inadvertently followed a twitter handle or have followed it for general intrigue, not because they believe the poster. What happens to them now? The cost is merely too high.

A number of travelers have reported searches that seem to violate the First Amendment. For instance, filmmaker Akram Shibly was ordered to hand over his phone password and social media names, and he claims officers also searched through his cloud-based applications.[253] Similarly, Jeremy Dupin, a Haitian journalist, claims the CBP searched through his reporting notes, information about his sources, and communications with his editors.[254]

C. GIVEN THAT SEARCHES OF ELECTRONIC DEVICES BURDEN THE FIRST AMENDMENT, CBP OFFICERS SHOULD BE REQUIRED TO HAVE PROBABLE CAUSE

The border search exception only applies to the Fourth Amendment—not the First Amendment. Thus, the protections of the First Amendment cannot be abrogated simply because the violations take place at the border. According to the controlling 2018 Directive, no suspicion is required for a basic search and only reasonable suspicion is required to perform an advanced search.[255] However, even a basic search by itself can reveal a substantial amount of protected information—twitter posts, emails sent and

252. *See Employers, Schools and Social Networking Privacy*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/other/employers-schools-and-social-networking-privacy (last visited July 19, 2019).

253. Farivar, *supra* note 32.

254. *Id.*

255. U.S. CUSTOMS & BORDER PROT., 2018 DIRECTIVE, *supra* note 19, at 4–5.

received, social media groups, photos, and much more—all without any bar of suspicion. Thus, to protect First Amendment rights and survive strict scrutiny, CBP officers must have probable cause to search an electronic device at the border—for both "basic" and "advanced" searches. Given that the Supreme Court has time and again protected the core principles behind the First Amendment, the CBP should recognize that its current policies cannot stand for various reasons including that there are less restrictive means to meet the government's interest, the burden on the First Amendment is too high and, in light of *Riley*, policies should be adjusted when concerning personal technology.

First, suspicionless searches should not be allowed when, as the Supreme Court has reiterated in cases of First Amendment issues, there is a less restrictive alternative the government can employ in order to meet its interests.[256] For electronic border searches, there is one: require probable cause for all searches. The state's interest is to collect evidence of those committing crimes and crossing the border. It fits that requiring probable cause of these crimes would be a less restrictive alternative, whereas searching any device is so restrictive and does not outweigh the chilling effects it has on First Amendment rights. As done with the Fourth Amendment and the border search exception, a balancing of state's interests can be used to decide what policies should be in place. Because First Amendment rights are so vital to our society, the policies must be much less intrusive than those currently in place. Additionally, because there are less intrusive ways to protect the border than to search through every phone—regardless of suspicion—the government should take alternative routes to protect First Amendment rights.

Second, the burden on First Amendment protections provided by these border searches is too high. Given the range of activity conducted on a device, a search of its contents and history can be highly invasive. For instance, an average smart phone has thirty-three installed applications that can reveal a "montage of the user's life."[257] Such unfettered access to one's device may chill free speech by threatening the safety and privacy of making use of such applications, websites, and emails in an otherwise legal way. For journalists traveling across the border, there is even more of a burden. For instance, these searches can have a chilling effect on a journalist's communication with a confidential source.[258]

256. *See, e.g.*, Denver Area Educ. Telcomms. Consortium, Inc. v. FCC, 518 U.S. 727, 741 (1996).
257. Riley v. California, 573 U.S. 373, 396 (2014).
258. Lana Sweeten-Shults, Opinion, *Anonymous Sources Vital to Journalism*, TIMES REC. NEWS,

Additionally, the encumbrance on anonymous speech and reading creates an unacceptable violation of the First Amendment. The Supreme Court, along with many scholars, has remarked on the importance of protecting people's safety in writing anonymously. This dates back to the Founding Fathers and the Federalist Papers and carries through to present day. If there is fear that a Twitter account discussing animal rights may be revealed and shared with other government arms, would someone censor him or herself when using the account? The supposed benefit of these searches—to discover communication between terrorists or uncover a child pornographer—is simply not outweighed by the chilling of speech caused by such searches. The ends simply do not meet the means. Our society relies on the ability to voice opinions anonymously and to not feel threatened when educating ourselves through reading. Simply put, the cost of fear of free speech is not enough to warrant suspicionless searches of any device, the copying of such information, the detention of such devices, nor the sharing of information with other government agencies without cause.

It is also important to protect free and anonymous association under the First Amendment. Today, with the advent of various technology platforms, there are many ways to easily associate oneself with a cause, group, person, and so on. These associations can be as simple as pressing a button on a social media account; however, the effect of being thus associated can sometimes create backlash. If each person's anonymous association—through, for example, an anonymous handle on Instagram—was open to easy government access, it would chill anonymous association.

Furthermore, as Justice Brennan commented in his concurrence in *Lamont*, "we cannot sustain an intrusion on First Amendment rights on the ground that the intrusion is only a minor one."[259] Although many may argue that searches of this kind on the border only slightly infringe on one's First Amendment rights, it is still an intrusion. And the justifications by the state are not enough to outweigh this intrusion to devices that hold almost all of our speech in the modern world.

While any search of the contents of electronic devices should be discontinued without probable cause or reasonable suspicion, searches of electronic devices' tangible and physical attributes can continue to fall within

https://www.timesrecordnews.com/story/opinion/columnists/lana-sweeten-shults/2017/02/27/anonymous-sources-vital-journalism/98481850 (last updated Feb. 28, 2017, 5:29 AM) ("Without [anonymous sources], journalists simply could not do their jobs. We would be relying on the official side of the story, and the official side of a story isn't always the whole side.").

259. Lamont v. Postmaster Gen., 381 U.S. 301, 309 (1965) (Brennan, J., concurring).

the border search exception. The physical keyboard or any papers stuffed into the pockets of an iPad case, for example, should continue to be searchable without suspicion under the border search exception because they are the same as a backpack or suitcase that has long been understood to fall under this exception.

Thus, given these burdens on the First Amendment's core principles, any digital search (whether basic or advanced) should be disallowed unless there is at least reasonable suspicion or probable cause. Following *Ickes*, in *Arnold* the defendant argued that there should be a reasonable suspicion standard—a higher level of suspicion—for searches that could uncover expressive material to protect First Amendment rights.[260] Even if we allow there to still be warrantless searches of electronic devices at the border and believe that the Fourth Amendment's border search exception should be extended, at the very least, the level of suspicion should be increased to protect First Amendment rights. Currently, the border search exception doctrine permits CBP officers to conduct a basic search of any property passing through the border, with or without suspicion.[261] However, even basic and manual searches of any electronic device should not be allowed unless the police reasonably suspect it contains evidence of a crime. In the digital age, the policy behind the First Amendment should protect electronic devices from the same procedure. The information in an electronic device is perceived to be more secure, anonymous and private than in any other forum. This perception prompts people to say, search, read, and share information they would not otherwise.

Lastly, the Supreme Court in *Riley* realized that policies should be adjusted with respect to electronic devices; this principle should be applied to border searches as well. Chief Justice Roberts, in his opinion holding that a cellphone should not be treated the same under Fourth Amendment as other physical property, claimed that:

> [T]here is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception.[262]

260. United States v. Arnold, 533 F.3d 1003, 1006 (9th Cir. 2008).

261. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

262. Riley v. California, 573 U.S. 373, 395 (2014). The Court also commented on how:

> There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps

Alternatively, courts can begin to draw a line between "invasive" searches of electronic devices in the way they have with body searches when it comes to the Fourth Amendment border exception doctrine. When it comes to searches of the person, the Third Circuit has said a mere patdown over clothes is routine and thus requires no suspicion whatsoever,[263] while, comparatively, a "skin search" requires a "real suspicion."[264] The courts have justified requiring a higher level of suspicion for a certain form of personal search but none for another by saying one form is more "intrusive" than the other and is therefore unreasonable.[265] Here, a search of a device in the early 2000s may not have been seen as that "intrusive" because the average device held very little information in comparison to today, and, therefore, it was easy for it to be reasonable and routine. Today, given the abundance of information on a device, a search of an electronic device should be considered invasive and provided the same protection as an above-the-clothes and skin search: a physical inspection of the devices physical properties requires no suspicion, while using the device to search requires a level of suspicion.

Looking forward, the district court's decision not to dismiss the First Amendment claim in the pending *Alasaad*[266] case provides support for the assertion that electronic devices are not subject to the full border search exception in the same way that electronic devices are not subject to the full search incident to arrest doctrine. Should this issue reach the Supreme Court, relying on its comments in *Riley*, the Court should find that electronic devices are different from other property and, thus, should be treated differently at the border.

CONCLUSION

In sum, the current procedures regarding border searches of electronic devices are unconstitutional in light of the First and Fifth Amendments. Thus, the CBP's policies must be rectified. First, CBP officers should no longer be able to ask, coerce, or threaten travelers in order to obtain

> for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.

Id. at 396.

263. Bradley v. United States, 299 F.3d 197, 203 (3d Cir. 2002).

264. United States v. Sosa, 469 F.2d 271, 272 (9th Cir. 1972).

265. *Bradley*, 299 F.3d at 204.

266. *See* Alasaad v. Nielsen, No. 17-cv-11730-DJC, 2018 U.S. Dist. LEXIS 78783, at *76 (D. Mass. May 9, 2018).

passwords or unlock devices. This practice violates the right against self-incrimination protected by the Fifth Amendment regardless of whether the CBP is asking for a traditional number, letter, and symbol password or for biometric authorization such as a fingerprint. If devices are protected by a security measure, it is up to the CBP to use its own abilities to unlock a device without asking an individual to do that for them. Furthermore, travelers should be notified of their right to refuse to provide CBP officers with authorization to their devices.

Second, searches of electronic devices should be limited to the physical casing of the device unless there is at least reasonable suspicion or a warrant. The chilling effect these suspicionless searches have on the core principles of the First Amendment make it too burdensome to continue. Current basic searches, which allow officers to scroll through devices such as a smartphone without even reasonable suspicion, should no longer be permitted. Reasonable suspicion should be the lowest bar needed to even look at the contents of a device being carried across the border. Advanced searches or forensic searches should be held to an even higher standard: probable cause.

Overall, the current directives and policies implemented and practiced by the CBP are unconstitutional.