THE YALE LAW JOURNAL FORUM
April 1, 2019

Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches

Laura K. Donohue

ABSTRACT. The warrantless search of travelers' electronic devices as they enter and exit the United States is rapidly increasing. While the Supreme Court has long recognized a border-search exception to the Fourth Amendment's warrant requirement, it applies to only two interests: promoting the duty regime and preventing contraband from entering the country; and ensuring that individuals are legally admitted. The government's recent use of the exception goes substantially beyond these matters. U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) are using it to search electronic devices, and at times the cloud, for evidence of *any* criminal activity, bypassing the warrant requirement altogether. Searches of these devices implicate privacy concerns well beyond those of the home, which has long been protected even for customs and immigration purposes. This Essay traces the evolution of the border exception, noting the effect of recent Supreme Court decisions, to argue that CBP and ICE are operating outside constitutional constraints. The Essay considers two objections grounded in the legitimate interests of CBP and ICE. It responds, first, that inspection of digital devices differs from the examination of a traveler's purse or luggage: the level of intrusion and the amount of information obtained changes the quality of the search, triggering Fourth Amendment protections. Second, as an immigration matter, as soon as citizens are identified, absent probable cause, the government does not have the constitutional authority to search their devices at all. Foreigners lacking a substantial connection to the country, however, do not enjoy the same Fourth Amendment protections. It concludes by observing that because of the substance and complexity of the issue, Congress has an important role to play in determining what types of searches are justified.

INTRODUCTION

Over the past three years, the warrantless search of travelers' electronic devices as they enter and exit the country has rapidly increased. In 2015, U.S. Customs and Border Protection (CBP) examined 8,503 devices. That number more than doubled the following year, before soaring in 2017 to more than 30,000

searches.[1] In 2015, U.S. Immigration and Customs Enforcement (ICE), in turn, reported the search of 4,444 cell phone and 320 other electronic devices. In 2016, ICE eclipsed these numbers, searching 23,000 devices.[2]

The Supreme Court has long recognized a border-search exception to the Fourth Amendment's warrant requirement. In *United States v. Flores-Montano*, the Court looked to the nation's sovereign "interest in protecting . . . its territorial integrity" to justify such searches.[3] In *United States v. Montoya de Hernandez*, the Court stated, somewhat more narrowly, that Congress is the source of the executive's power. It explained that "[s]ince the founding of our Republic . . . [Congress has] granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant."[4] The Commerce Clause permits Congress to authorize the seizure of goods at the border.[5]

Congress and the courts endorsed only two justifications for broad border search authorities: first, "to regulate the collection of duties and to prevent the introduction of contraband into this country;"[6] and, second, to ascertain which

1. *See* U.S. CUSTOMS & BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf [https://perma.cc/2EA3-NEFR] [hereinafter CBP DIRECTIVE]; *CBP Releases Statistics on Electronic Device Searches*, U.S. CUSTOMS & BORDER PROTECTION (Apr. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0 [https://perma.cc/35KZ-XLEM]; *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. CUSTOMS & BORDER PROTECTION (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and [https://perma.cc/2QHN-22YD].

2. Daniel Victor, *What Are Your Rights if Border Agents Want to Search Your Phone?*, N.Y. TIMES (Feb. 14, 2017), https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html [https://perma.cc/7VHT-GPTB].

3. United States v. Flores-Montano, 541 U.S. 149, 153 (2004); *see also* Torres v. Puerto Rico, 442 U.S. 465, 472-73 (1979) ("The authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity. By reason of that authority, it is entitled to require that whoever seeks entry must establish the right to enter and to bring into the country whatever he may carry.").

4. United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

5. *See, e.g.*, United States v. 12 200-Ft. Reels of Super 8MM. Film, 413 U.S. 123, 125 (1973) ("[S]earches of persons and packages at the national borders rest on different considerations . . . from domestic regulations. The Constitution gives Congress broad, comprehensive powers '[t]o regulate commerce with foreign Nations.' . . . Historically, such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry." (citations omitted)).

6. *Montoya de Hernandez*, 473 U.S. at 537; *see also* Act of July 31, 1789, ch. 5, 1 Stat. 29, *repealed by* Act of Aug. 4, 1790, ch. 35, § 73, 2 Stat. 177; Carroll v. United States, 267 U.S. 132, 147-51 (1925); Boyd v. United States, 116 U.S. 616, 623 (1886).

persons should be admitted to the United States.[7] For the latter, ensuring proper legal process (and immigration status) proved paramount.[8] Looking to these areas, Congress empowered the executive to monitor "who and what may enter the country."[9] Congress did *not* provide an exception for ordinary law enforcement to use the movement of people to look for evidence of criminal activity. To the contrary, only customs agents and immigration officials could exercise authorities narrowly tailored to intercept contraband and control immigration.

Current electronic border searches eclipse the traditional limits placed on the executive to justify the departure from Fourth Amendment requirements. CBP and ICE search devices for any criminal activity, with no limits on use of the material in subsequent proceedings.[10] The executive branch, moreover, has targeted individuals, using their movement across frontiers to obtain information that otherwise would require a warrant to access.[11] Thus far, the courts have provided something of a backstop, chastising the executive in some of the more

---

7. *See infra* Parts III and IV (tracing the purposes of broader search authorities at the border back to the founding of the Republic).

8. A third area, disease prevention, also justified search powers. Such considerations are not immediately relevant to the discussion regarding searches of electronic devices, although the examination of certain types of information on such devices could raise parallel concerns. For further discussion of the evolution of quarantine authorities, see Laura K. Donohue, *Pandemic Disease, Biological Weapons, and War, in* LAW AND WAR 84 (Austin Sarat et al. eds., 2014); and Laura K. Donohue, *Biodefense and Constitutional Constraints*, 4 NAT'L SEC. & ARMED CONFLICT L. REV. 82 (2014).

9. United States v. Ramsey, 431 U.S. 606, 620 (1977).

10. *See, e.g.*, U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, ICE DIRECTIVE No. 7-6.1: BORDER SEARCHES OF ELECTRONIC DEVICES, para. 8.5(1)(a) (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf [https://perma.cc/MAP7-QL82] [hereinafter 2009 ICE DIRECTIVE] (allowing for the seizure and retention of electronic devices or copies of information held on them when there is evidence of any "unlawful activity"); *id* (allowing ICE to share any information obtained "with Federal, state, local, and foreign law enforcement agencies"); *Inspection of Electronic Devices*, U.S. CUSTOMS & BORDER PROTECTION, https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf [https://perma.cc/W5T4-FASY] [hereinafter *Inspection of Electronic Devices*] ("If CBP determines . . . the device contains evidence of a crime, contraband or other prohibited or restricted items of information—then you will be notified of the seizure."); *Policy Regarding Border Search of Information*, U.S. CUSTOMS & BORDER PROTECTION (July 16, 2008), https://www.cbp.gov/sites/default/files/documents/search_authority_2.pdf [https://perma.cc/8KW9-KFMN] ("[O]fficers may examine documents, books, pamphlets, and other printed material, as well as computers, disks, hard drives, and other electronic or digital storage devices. These examinations are part of CBP's longstanding practice and are essential to uncovering vital law enforcement information.").

11. *See, e.g.*, Alasaad v. Nielsen, No. 17-CV-11730-DJC, 2018 WL 2170323 (D. Mass. May 9, 2018); Sixth Joint Status Report, Knight First Amendment Inst. at Columbia Univ. v. Dep't of Homeland Sec., No. 1:17-CV-00548-TSC (D.D.C. May 21, 2018) (summarizing FOIA litigation that revealed hundreds of complaints filed by individuals whose devices were searched at

egregious cases.[12] But in an increasingly globalized world in which citizens' border crossings repeatedly expose them to intrusive government searches, the lack of Supreme Court attention and statutory law is of concern. It leaves rights at the mercy of each agency's regulatory regime. As the Court recognized in *Riley v. California*, "the Founders did not fight a revolution to gain the right to government agency protocols."[13]

The rights at stake are substantial. Electronic devices "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[14] Even the term "cell phone" is misleading, as "many of these devices are in fact minicomputers that also happen . . . to be used as a telephone."[15] Their distinguishing feature is the "immense storage capacity."[16] As the Court noted, "[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read."[17] With mobile devices, they can. The search of electronic devices differs from luggage searches in terms of volume as well as the *type* of information that can be obtained: medical records, location data, information regarding political beliefs or religious convictions, and details about intimate relationships — stretching back for decades. Further, electronic devices also provide a gateway to digital information stored in the cloud.[18]

---

the border); *see also* Brief of the Knight First Amendment Institute at Columbia University and the Reporters Committee for Freedom of the Press as Amici Curiae Supporting Plaintiffs, *Alasaad*, 2018 WL 2170323 (arguing that the search policies violated the First and Fourth Amendments).

12. *See, e.g.*, United States v. Kim, 103 F. Supp. 3d 32, 54 (D.D.C. 2015) (rejecting a mechanical approach to allowing warrantless searches for digital content on cell phones).

13. 134 S. Ct. 2473, 2491 (2014).

14. *Id.* at 2488-89.

15. *Id.* at 2489.

16. *Id.*

17. *Id.*

18. This occurs in two primary ways: first, by using the devices to access network information, and, second, by requiring travelers to provide identifiers or handles, or account login credentials (such as usernames and passwords) to access social media. The latter presented in December 2016 when CBP started asking non-U.S. persons entering the country under the Visa Waiver Program (VWP) to disclose their social media identifiers. (Under the VWP, foreign citizens can visit the United States for up to ninety days without a visa if they have been cleared by the Electronic System for Travel Authorization.) Initially, the program was voluntary and focused on publicly-available information. In January 2017, however, the Council on American-Islamic Relations (CAIR) filed complaints with the U.S. Department of Homeland Security, alleging that citizens were being directed to disclose not just the passwords to their phones, but also their social media login information. *CAIR-FL Files 10 Complaints with CBP After the Agency Targeted and Questioned American-Muslims About Religious and Political Views,* CAIR FLORIDA (Jan. 18, 2017), https://www.cairflorida.org/newsroom/press-releases/720

A search of mobile devices compromises far more detailed and personal information than a search of an individual's home, which traditionally has received the highest protections under the Fourth Amendment.[19] For the latter, a warrant must describe with particularity what is being sought based on probable cause of involvement in specific crimes. Officers cannot simply cast about looking for any potential criminal activity. Search of an electronic device, though, allows law enforcement to scour countless areas of an individual's life. It is the equivalent of looking not just at an individual's home, but entering their bank, their car, and their workplace; accompanying them on dates and on social occasions; going to the PTA meeting with them, or to their local grocery store or mall; attending their places of worship; and sitting down next to them at the public library to make a record of everything they read.

Home warrants also are particularized in their execution against named individuals. In contrast, the search of an electronic device uncovers lots of data about extended family, friends, and acquaintances. Metadata pinpoints them at certain places at particular times. Otherwise password-protected social media

-cair-fl-files-10-complaints-with-cbp-after-the-agency-targeted-and-questioned-american-muslims-about-religious-and-political-views.html [https://perma.cc/5BZZ-9KTA]; *see also* Sophia Cope, *Fear Materialized: Border Agents Demand Social Media Data from Americans*, ELECTRONIC FRONTIER FOUND. (Jan. 25, 2017), https://www.eff.org/deeplinks/2017/01/fear-materialized-border-agents-demand-social-media-data-americans [https://perma.cc/SYT2-6Z8N] (criticizing the CBP's social media policy). Media reported that officials were considering new policies to expand CBP scrutiny of cloud content. In February 2017, newly-appointed DHS Secretary John Kelly told a congressional committee that the agency might adopt a provision requiring login information from all foreign visa applicants, with failure to comply resulting in denial of entry. Starting in May 2017, login information became required in cases tied to national security. Less than a year later, in March 2018, the U.S. Department of State submitted a formal proposal to the Office of Management and Budget, requiring that almost all visa applicants list all social media identities used over the previous five years, all telephone numbers, all email addresses, all international travel, all prior immigration violations, and whether specified family members have been involved in terrorist activity. 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa, 83 Fed. Reg. 13807 (proposed Mar. 30, 2018). The rule change would allow the government to vet and identify about 14.7 million people per year, searching any social media platforms associated with the individual. Matthew Lee, *U.S. to Seek Social Media Details from All Visa Applicants,* BLOOMBERG (Mar. 29, 2018), https://www.bloomberg.com/news/articles/2018-03-29/us-to-seek-social-media-details-from-all-visa-applicants; Brendan O'Brien, *U.S. Visa Applicants to Be Asked for Social Media History: State Department*, REUTERS (Mar. 30, 2018), https://www.reuters.com/article/us-usa-immigration-visa/u-s-visa-applicants-to-be-asked-for-social-media-history-state-department-idUSKBN1H611P [https://perma.cc/HSE5-ZWDR].

19. Since before the Founding, outside the fleeing felon and the hue and cry, a particularized warrant has been required to access the home. *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181 (2016).

accounts reveal what they know and believe, what they find amusing—or upsetting, and what their political views may be. Intimate thoughts, conveyed through email, remain even *after* users delete messages. Access to all of this stretches, potentially, years backwards in time.

As a substantive matter, what is present in a house or apartment is more limited than what can be obtained from the search of a mobile phone or computer. Inside the home, business records are far less likely to be found than at work. Financial data is bounded by time and records retention. Correspondence, at best, will be incomplete, and photographs generally will be only those that have been printed. In comparison, one phone may contain and provide access to all of an individual's work documents (as well as some of their colleagues'), complete financial records, extensive correspondence, and *every* photo ever taken. From this, the number and quality of an individual's intimate relationships can be discovered, and the strength of an individual's social networks ascertained. Inside the home, there may only be traces of where an individual has gone outside the home (perhaps because of a souvenir here or there). On the phone, however, this information may be stored in map applications, address books, photograph and video metadata, and GPS records. A private library does not contain every book an individual has read. Electronic devices, in contrast, capture *all* digital print books, audio books, and internet-based materials an individual has read, as well as movies they have watched, jokes at which they've laughed, and statements made on social media with which they agree. This is far more information than law enforcement would be able to obtain by executing a physical warrant. By accessing a phone, moreover, if certain applications have been downloaded, law enforcement could gain access not just to the digital world, but also to the inside of the home itself.[20]

This Essay argues that the electronic searches CBP and ICE are conducting at ports of entry violate the Fourth Amendment. It documents the well-established, historical limitations on border searches that have served to justify the exception, and demonstrates how current practices fall well outside constitutional protections.[21] It begins with the current CBP and ICE regulations that

20. For instance, Blink Home Monitor, an application that can be downloaded to smartphones and tablets, provides homeowners with real-time coverage of what is happening inside their houses. If CBP or ICE were to search a mobile device and open the application, they could (virtually) enter someone's home as they cross the border. *See Blink Home Monitor Smartphone and Tablet Apps*, BLINK, https://blinkforhome.com/pages/blink-home-monitor-app?locale=en [https://perma.cc/L2VL-ZCNA].

21. While this Essay focuses on the Fourth Amendment, the rights of free speech, free association, and freedom of religion are also implicated by border searches. These rights "are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference." Bates v. City of Little Rock, 361 U.S. 516, 523 (1960); *see also* Memorandum and Order, Alasaad v. Nielsen, No. 17-CV-11730-DJC, 2018 WL 2170323, at *22 (D.

govern the search of travelers' devices before laying out the history of customs border search authorities, observing that the primary purpose of these measures is and has always been to interdict contraband and to prevent uncustomed goods from entering the country. These limited aims, which relate to sovereignty, form the core justification behind the border search exception. Here, strong protections have been extended to the home, even where contraband may be at issue.

Mass. May 9, 2018). Compulsory "disclosure of political affiliations and activities can impose just as substantial a burden on First Amendment rights as can direct regulation." AFL-CIO v. Fed. Election Comm'n, 333 F.3d 168, 175 (D.C. Cir. 2003); *see also* Memorandum and Order, *Alasaad*, 2018 WL 2170323, at *22. Therefore, "[w]hen a State seeks to inquire about an individual's beliefs and associations a heavy burden lies upon it to show that the inquiry is necessary to protect a legitimate state interest." Baird v. State Bar of Ariz., 401 U.S. 1, 6-7 (1971); *see also* Memorandum and Order, *Alasaad*, 2018 WL 2170323, at *22. Electronic media, in particular, falls within First Amendment protections. Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017). Justice Kennedy observed: "[w]hile in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear . . . [i]t is cyberspace – the 'vast democratic forums of the internet' in general, and social media in particular." 137 S. Ct. at 1735 (quoting Reno v. ACLU, 521 U.S. 844 (1997)). He added, "[social media] websites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard." *Id.* The implications of access to electronic devices for religious freedom, free speech, and free association are substantial. Information contained in mobile phones, tablets, and computers implicates the most intimate aspects of a person's politics, beliefs, and relationships. In *Alasaad v. Nielsen*, the court has acknowledged the strength of the First Amendment claims. Litigants in that case (on behalf of eleven travelers) seek an injunction against DHS, CBP, and ICE and the expungement of private information that was obtained in multiple prior warrantless electronic border searches. Memorandum and Order, *Alasaad*, 2018 WL 2170323, at *10-16. The government's initial effort to have the case dismissed on Fourth and First Amendment grounds failed. *Id.* As a matter of Fourth Amendment law, the district court "concluded that *Riley* has some weight in the border search context," thus establishing "a plausible Fourth Amendment claim." *Id.* at *21; *see also* Memorandum in Support of Defendants' Motion to Dismiss, *Alasaad*, 2017 WL 6998925, at *15-27 (D. Mass. Dec. 15, 2017). Although the district court in *Alasaad* did not agree with the plaintiffs that strict scrutiny was warranted (on the grounds that CBP and ICE policies are content-neutral), it recognized that compelled disclosure "cannot be justified by a mere showing of some legitimate governmental interest." Memorandum and Order, *Alasaad*, 2018 WL 2170323, at *22 (quoting Buckley v. Valeo, 424 U.S. 1, 64 (1976)). First Amendment doctrine requires a "substantial relation between the governmental interest and the information required to be disclosed." *Id.* (quoting Buckley, 424 U.S. at 64-65). The court noted that the plaintiffs had argued that in light of the immense storage capacity of both electronic devices and the cloud, the regulations "impose a substantial burden on First Amendment rights without justification." *Id.* (brackets and internal quotation marks omitted). Instead of countering the plaintiffs' claim, the government had merely stated that a First Amendment exception to border search doctrine would be "staggering." *Id.* at *23 (quoting United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005)). The court rejected the government's assumption that all expressive material would thereby be excluded, suggesting that the plaintiffs had raised a plausible claim that the current policies "unjustifiably burden travelers' First Amendment rights." *Id.*

The Essay then turns to the evolution of immigration law, pointing out that the historical purpose of such measures has been (a) to establish identity, (b) to admit "desirable" aliens, and (c) to exclude others, subject to policies set by Congress. The only reason the border search exception applies at all is to permit Congress to achieve these objectives. Even then, the powers of search and seizure are subject to higher protections at the threshold of the home.

The Essay next focuses on Fourth Amendment doctrine, looking at how the circuit courts have come down on the question of electronic border searches before and after a string of recent Supreme Court cases challenging traditional doctrine: *Riley*,[22] *United States v. Jones*,[23] and *Carpenter v. United States*.[24] Applying the two-part approach articulated by Chief Justice Roberts in *Carpenter*, which focused on the nature of the documents being sought and limitations on any legitimate expectations of privacy regarding the contents, this Part recognizes that the border search exception does not apply to electronic devices in the same way it does to the search of a traveler's other belongings.[25]

The government considers its current practices constitutional in light of the status of electronic data as a form of "digital contraband".[26] The Essay responds with two arguments. First, just as bits and bytes constitute the functional equivalent of illegal material, so, too, does the search that is being undertaken represent the functional equivalent of the search of the home, and, potentially, every aspect of an individual's life. For the same reasons that the Court in *Riley* rejected the search of electronic devices within U.S. borders, examination of the same at ports of entry constitutes precisely the type of search covered by the Fourth Amendment and, historically protected *even in the context of customs and duties*. Second, to the extent that one could argue that criminals could take advantage of such a rule to upload material to the cloud, cross the border, and then download it within the U.S. (thereby avoiding detection), in-person physical transit has never been a necessary to bring contraband into the United States. Where sent through the post, Fourth Amendment protections still apply. Additionally, in a digital world, it is not only as a traveler crosses the border that the government has an opportunity to intercept material. Electronic search provisions, recent changes to the Federal Rules of Criminal Procedure, and foreign intelligence

22. 134 S. Ct. 2473 (2014).

23. 565 U.S. 400 (2012).

24. 138 S. Ct. 2206 (2018).

25. *Id.* at 2218-20 (addressing (a) the nature of the documents being sought; and (b) limitations on any legitimate expectations of privacy in the information).

26. *See, e.g.*, Government's Opening Brief at 49, United States v. Arnold, 2007 WL 1407234 (9th Cir. Mar. 29, 2007) (No. 06-50581) ("The court's decision therefore poses a serious risk of affirmatively increasing the use of computers as a sanctuary for digital contraband and other harmful materials.").

authorities allow the government to identify illegal activities, conduct investigations, and access digital materials. At the border, a gradated search that distinguishes between reasonable suspicion for a basic (manual) search and probable cause for an advanced, forensic search would recognize that some level of suspicion is required at the outset to search devices, and that such searches ought not to be granted in toto, but should take place under narrowly-circumscribed limits absent the stronger showing of probable cause. Where such matters enter the domain of matters ordinarily encased in the home, the Fourth Amendment establishes more stringent protections.

The Essay also addresses the primary counterargument regarding immigration measures: that it is the role of immigration authorities to identify and to inquire into the type of person admitted to the United States. In response, it notes that U.S. persons, as soon as their identity as citizen or legal resident is established, are no longer subject to immigration search authorities. Thus, *no search of U.S. persons' electronic devices* is justified under the immigration exception. For non-U.S. persons, who lack a substantial relationship to the United States, CPB and ICE have broader authority. One of the starkest examples of how the current regulations fail to provide adequate protections is in the realm of electronic communications, where, despite the use of passwords and encryption, travelers are denied *the same privacies* that would be extended to *the same material* if it were physically written on paper. The Essay concludes by reiterating the concern that current practices violate constitutional norms, acknowledging that once a traveler establishes their citizenship, their electronic devices can only be searched consistent with the Fourth Amendment probable cause and warrant requirements, and proposing a stronger role for Congress in developing a statutory regime for noncitizens seeking entry.

I. CURRENT REGULATORY REGIME

The rights at issue in the government's search of electronic devices at the border are substantial. Even so, these searches are governed by agency regulations that do not account for the importance of the interests at stake. This Part briefly describes the existing regime.

CBP's January 2018 guidelines allow for "basic" searches without suspicion.[27] This means that the agency considers itself entitled to seize the mobile phones,

27. *See* CBP DIRECTIVE, *supra* note 1. The Trade Facilitation and Trade Enforcement Act of 2015 required CBP to establish "standard operating procedures for searching, reviewing, retaining, and sharing information contained in communication, electronic, or digital devices encountered . . . [at] ports of entry." Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. No. 114-125, § 802(a), 130 Stat. 122, 205 (codified at 6 U.S.C. § 211(k)(1)(A) (2018)). The statute requires CBP to update its procedures every three years.

tablets, and laptops of every U.S. citizen—including those of judges, Justices, and Members of Congress, and their colleagues, families and friends—without any suspicion of wrongdoing. With one exception, there are no statutory, regulatory, or, according to the agencies, constitutional limits on who can see this information, how long it can be kept, or how it can be used.[28] For attorney-client-privileged material, or attorney work product, a "filter team" segregates protected material.[29] There are no special protections provided for journalists, sensitive political material, trade secrets, medical information, or materials otherwise privileged at law. Information obtained from these searches can be shared with any federal, state, local, or foreign law enforcement agency.[30] For "advanced" forensic searches, which involve connecting external equipment "to an electronic device not merely to gain access . . . but to review, copy, and/or analyze its contents," [31] customs officers must merely meet a standard of "reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern."[32]

In December 2018, the Department of Justice Office of Inspector General released a report on CBP's border searches, finding that the agency had violated its own guidelines by failing to limit its collection of electronic data and to delete information obtained.[33] The problem was widespread: sixty-seven percent of the Electronic Media Reports examined contained inconsistencies.[34] Officials

---

28. *See, e.g.*, 19 U.S.C. § 1467 (2018) (empowering customs officers to inspect, examine, and search persons, baggage, and merchandise without limiting subsequent use of what is discovered); 19 U.S.C. § 1581(a) (2018) (empowering officials to examine, inspect, and search vessels or vehicles without restriction on subsequent use); 19 U.S.C. § 1582 (2018) (empowering the Secretary of the Treasury to issue regulations for searching persons and baggage); *see also* 19 U.S.C. § 1496 (2018) (empowering customs officers to examine the baggage of any person arriving in the United States); 19 U.S.C. § 1499 (2018) (specifying procedures for the inspection, appraisement, and examination of imported merchandise).

29. CBP DIRECTIVE, *supra* note 1, at 10 para. 5.2.1.2.

30. *Id.* at 10 para. 5.5.1.3.

31. *Id.* at 5 para. 5.1.4.

32. *Id.* Critics raise concern that manual searches can be just as intrusive as forensic searches, with the implication that the type of information at stake (all emails, text messages, contacts, photos, calendar items, browsing histories, and the like) meets the threshold for a warrant requirement. *See, e.g.,* 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 [https://perma.cc/RW5Y-HT5P]. They also note that at the border, "national security" can be broadly construed, proving an exception to the rule. *Id.*

33. OFFICE OF THE INSPECTOR GENERAL, DEP'T HOMELAND SEC., CBP'S SEARCHES OF ELECTRONIC DEVICES AT PORTS OF ENTRY – REDACTED 5, 8-9 (2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-12/OIG-19-10-Nov18.pdf [https://perma.cc/H2FN-SUWX].

34. *Id.* at 6.

had consistently failed, for instance, to disable data connections to networks prior to search of the devices; other information was simply copied onto thumb drives and kept.[35] Although the 2018 *Privacy Impact Assessment for CBP Border Searches of Electronic Devices* stated that the Department of Homeland Security (DHS) should audit the agency's collection of personally-identifiable information, nothing has yet been made publicly available.[36]

The equivalent 2009 ICE directive has not been updated since the last review in 2012.[37] Like its CBP counterpart, the mandate applies to any item containing electronic or digital information.[38] However, there are three critical differences which, as a formal matter, empower ICE to conduct even more intrusive searches. First, the document authorizes ICE Special Agents to "search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion."[39] In the course of the search, the policy explicitly protects agents' authority "to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems."[40] Second, there is no heightened standard imposed for forensic searches. Instead, "[a]t any point during a border search, electronic devices, or copies of information therefrom, may be detained for further review either on-site at the place of detention or at an off-site location."[41] Searches can take place up to thirty days after the information is seized, with continuations subject to supervisory approval every fifteen days thereafter.[42] Third, unlike

35. *Id*.

36. *See* U.S. DEP'T HOMELAND SEC., DHS/CBP/PIA-008(A), PRIVACY IMPACT ASSESSMENT UPDATE FOR CBP BORDER SEARCHES OF ELECTRONIC DEVICES 20 (2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp008-bordersearcheselectronicdevices-january2018.pdf [https://perma.cc/HJK9-V657]; *see also* Complaint for Injunctive Relief at 6, Electronic Privacy Information Center v. U.S. Customs and Border Protection, No. 1:19-cv-00279 (D.D.C. Feb. 1, 2019), https://epic.org/foia/cbp/border-device-search-audits/Complaint.pdf [https://perma.cc/FKU4-CZKT].

37. 2009 ICE Directive, *supra* note 10.

38. *Compare id.* at 2 para. 5.2 ("Any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices."), *with* CBP DIRECTIVE, *supra* note 1, at 2 para. 3.2 ("Any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.").

39. 2009 ICE Directive, *supra* note 10, at 2 para. 6.1.

40. *Id.* at 2 para. 6.3.

41. *Id*. at 4 para. 8.1.4.

42. *Id*. at 5 para. 8.3.1.

CBP, which (ostensibly) only performs basic searches in the equivalent of "airplane mode," ICE can access information held on the cloud.[43]

The disjunction between CBP and ICE to some extent reflects their respective streams of authority: customs and immigration. The former emphasizes finding contraband, while the latter focuses on the character of individuals entering the country—partially explaining ICE's broader search powers in regard to online information and data stored on the cloud. Regardless, both agencies' actions are merging into the realm of traditional law enforcement, raising troubling constitutional concerns.

II. CUSTOMS BORDER SEARCH AUTHORITIES

Historically, the executive branch had latitude to conduct searches at the border without first establishing probable cause and obtaining a warrant. The breadth of that authority derived in part from the evolution of customs law. During the early colonial period, England understood customs searches as necessary in the context of commercial regulation, as customs provided an opportunity to ensure dominance in shipping and trade. Over time, the emphasis shifted to using customs to generate revenue. Officials thus obtained broad powers to search for, and to interdict, "uncustomed" materials. Following the American Revolution, the latter emphasis survived, laying the groundwork for today's CBP authorities. This history matters: it demonstrates that the purpose of customs search authority is to generate revenue and to interdict contraband. Where such searches moved away from the border and entered onto private property, special protections applied. Both aspects—the purpose of the search and the restrictions applied in relation to the home—serve as a limit on the border search exception.

A. Colonial History: Commercial Regulation Versus Revenue Generation

England saw in the American colonies an opportunity to consolidate its dominance in global shipping and trade. Accordingly, the customs laws applied to the colonies initially focused on goods shipped to and from the Americas, requiring, first, that they be brought to England and, later, carried exclusively on English vessels.

As early as 1621, the Privy Council recognized the financial and commercial opportunities at stake, arguing that "the Commodities brought from" the colony of Virginia ought to be "appropriated unto his Majesties subjectes" instead of

43. *Compare id.* at 2 para. 6.1, *with* CBP DIRECTIVE, *supra* note 1, at 4 para. 5.1.2 ("Officers may not intentionally use the device to access information that is solely stored remotely.").

being "communicated to forraine countries."[44] The council accordingly adopted an ordinance requiring that "all Tobacco and other commodities" from Virginia shall "not be carried into any forraine partes until the same have beene first landed here and his Majesties Customes paid therefore."[45] In the first Navigation Act of 1651, Parliament went on to require that any materials to or from the Americas be carried on English ships.[46] The goal was to prevent European powers from trading directly with the colonies.

Following the Stuart Restoration, in 1660 Parliament passed the second Navigation Act, re-entrenching the rule that colonial trade be carried out only on English vessels. The vessels had to be English-owned, operated by an English master, and carry a crew of which three-quarters must be English.[47] The statute did not prevent foreign imports to the colonies—it merely required transport under the English flag. Three years later, Parliament tightened its grip with the third Navigation Act, requiring that any European commodities bound for the colonies first be taken to England, unloaded, and duties paid, prior to their return to North America.[48] The goal was to establish a monopoly over colonial trade.

Over time, English statutes applied to the colonies shifted their focus from commercial regulation to revenue generation. The early navigation statutes erroneously assumed that most or all colonial trade involved overseas commerce.[49] In the absence of regulation, intracolonial trade (not subject to duties) began to flourish, with commodities eventually making their way to Europe "to the great hurt and diminution of the Customs and of the trade."[50] Parliament closed this gap in the Navigation Act of 1673, requiring that a bond be paid on enumerated items where the ship travelled between plantations.[51] The enforcement devices, though, were weak. They also differed from those in place in England: in the late seventeenth century, customs agents could search

---

44. THOMAS C. BARROW, TRADE AND EMPIRE: THE BRITISH CUSTOMS SERVICE IN COLONIAL AMERICA 1660-1775, at 4 (1999).

45. *Id.*

46. An Act for Increase of Shipping, and Encouragement of the Navigation of this Nation, (1651), 2 ACTS & ORDS. INTERREGNUM, 1642-1660, at 559 (C.H. Firth & R.S. Rait eds., 1911).

47. Navigation Act 1660, 12 Car. 2 c. 18 (Eng.).

48. Navigation Act 1663, 15 Car. 2 c. 7 (Eng.).

49. BARROW, *supra* note 44, at 6.

50. *Entry Book: Miscellaneous Years, 1689-92*, 9 CALENDAR TREASURY BOOKS 1960, 1965 (William A. Shaw ed., 1931), http://www.british-history.ac.uk/search/series/cal-treasury-books [https://perma.cc/FAG5-A6KQ] [hereinafter C.T.B.].

51. Navigation Act 1673, 25 Car. 2 c. 7 (Eng.).

"any ship, house, or place soever" in London to search for prohibited goods.[52] The Treasurer could provide a warrant to the customs commissions to examine trunks and boxes held at the Custom House in Southampton.[53] There was no colonial equivalent.

Accordingly, in the eighteenth century, Britain assumed greater powers to search for, and to seize, colonial contraband.[54] Lord Grenville, the First Lord of the Treasury, and Chancellor of the Exchequer, famously considered the colonies to be the best source of revenue, charging the colonies with a failure to offset the costs of their own defense.[55] He repeatedly argued in Westminster for more stringent customs enforcement in North America. Many agreed, so when the Molasses Act expired, Parliament passed a measure that emphasized mercantilism and revenue generation. The preamble to the American Revenue Act of 1764, otherwise known as the Sugar Act, explained: "[I]t is expedient that new provisions and regulations should be established for improving the revenue of this kingdom, and for extending and securing the navigation and commerce between Great Britain and your Majesty's dominions in America."[56] This statute, along with the Currency Act of 1764[57] (in which Britain assumed control of the colonial system of currency), laid the groundwork for the revolt that followed the introduction of the Stamp Act of 1765.[58]

B. Contraband in the Early American Republic

Following independence, when the United States found itself in need of revenue to pay for the war, customs inspectors continued to have broad search authorities. The fledgling country needed efficient customs enforcement mechanisms. Contraband meant a loss of revenues. Thus, from the earliest days

---

52. *Compare Entry Book: October 1663*, *in* 1 C.T.B., *supra* note 50, at 547, 550, *with Entry Book: December 1661*, *in* 1 C.T.B., *supra* note 50, at 311, 315 (directing John Seymour and Charles Smith "to search for all wares and merchandize mentioned in the royal proclamation of November 20 last for prohibiting the importation of divers foreign wares and merchandizes into this realm of England and Wales").

53. *Entry Book: April 1661*, *in* 1 C.T.B., *supra* note 50, at 232, 238.

54. *See generally* GAUTHAM RAO, NATIONAL DUTIES: CUSTOM HOUSES AND THE MAKING OF THE AMERICAN STATE (Edward Gray et al. eds., 2016).

55. Philip Lawson, *George Grenville and America: The Years of Opposition, 1765 to 1770*, 37 WM. & MARY Q. 561, 568 (1980).

56. The Sugar Act 1764, 4 Geo 3 c.15 (Gr. Brit.). *See* FRED ANDERSON, *The American Duties Act (The Sugar Act)*, *in* CRUCIBLE OF WAR: THE SEVEN YEARS' WAR AND THE FATE OF EMPIRE IN BRITISH NORTH AMERICA, 1754-1766, at 572 (2000).

57. Currency Act 1764, 4 Geo. III c. 34 (Eng.).

58. Duties in American Colonies Act 1765, 5 Geo. III c. 12 (Eng.).

of the Republic, customs inspectors could board vessels to search for contraband without first obtaining a warrant. To find the same items within a dwelling house, building, or other place, though, customs officers first had to obtain a warrant based upon "cause to suspect."[59]

In 1789, the same year that Congress forwarded the Bill of Rights to the states for ratification, it enacted statutes setting duties, establishing international ports of entry, requiring vessels to report their contents, and providing for inspectors to board vessels to examine whether the stated goods comported with the items on board.[60] Under the Act of July 31, 1789, officials could board any vessel "in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed; and therein to search for, seize, and secure any such goods, wares or merchandise."[61] The statute drew a line at the threshold of the home: where agents suspected that such materials were concealed in a "dwelling house, store, building, or other place," they could apply to a justice of the peace *for a warrant* to conduct a search for the goods, "and if any shall be found, to seize and secure the same for trial."[62] Congress passed

---

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

60. An Act for laying a Duty on Goods, Wares, and Merchandises imported into the United States, ch. 2, §§ 1, 3, 4, 1 Stat. 24, 24-27 (1789) (setting duties); An Act to regulate the Collection of the Duties imposed by law on the tonnage of ships or vessels, and on goods, wares and merchandises imported into the United States, Act of July 31, 1789, ch. 5. § 1, 1 Stat. 29, 29 (establishing districts, ports, and officers); *id.* § 2 (establishing ports for non-U.S. vessels); *id.* § 4 (requiring the master or commander of every ship or vessel to provide "a true manifest of the cargo on board such ship or vessel"); *id.* § 5 (empowering the inspectors of vessels "to examine whether the goods imported are conformable to the entries thereof"); *id.* § 10 (requiring that the master or commander of the vessel to provide the manifest to the inspector with "a true account of the loading which such ship or vessel had on board at the port from which she last sailed, and at the time of her sailing, or at any time since, the packages, marks and numbers, and noting thereon to what port in the United States such ship or vessel is bound, and the name or names of the person or persons to whom the goods are consigned, or in cases where the goods are shipped to order, the names of the shippers"); *id.* § 12 (prohibiting any goods, wares, or merchandise from being unladen or delivered from any ship or vessel at night or without a permit from the collector); An Act for Registering and Clearing Vessels, Regulating the Coasting Trade, and for other purposes, ch. 11, § 3, 1 Stat. 55, 55-56 (1789) (empowering the surveyor to measure every vessel to ascertain its tonnage); An Act to suspend part of an Act, intituled 'An Act to regulate the collection of the Duties imposed by Law on the Tonnage of Ships or Vessels, and on Goods, Wares, and Merchandises, imported into the United States,' and for other purposes, ch. 15, § 3, 1 Stat. 69, 69-70 (1789) (setting duties on certain foreign goods).

61. An Act to regulate the Collection of the Duties imposed by law on the tonnage of ships or vessels, and on goods, wares and merchandises imported into the United States, ch. 5, § 24, 1 Stat. 29, 43 (1789) (codified at 19 U.S.C § 482 (2018)).

62. *Id.*

additional statutes in 1790, 1793, and 1799, all of which underscored the importance of the enforcement of duties.[63]

Contemporaneous with the drafting and adoption of the Fourth Amendment, the First, Second, and Fourth Congresses signaled that there was no need to obtain a warrant for goods subject to forfeiture when held in a ship or vessel. The amendment did not include any exceptions in the text, but the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable search and seizure" applied to domestic matters—not to goods crossing the border.[64] Once such goods, however, were held in a warehouse, building, or dwelling *within* the United States, the law required that customs agents obtain a warrant before conducting a search.

Vehicles and goods in transit presented a particular conundrum, which Congress addressed in the Act of July 18, 1866.[65] That statute made it lawful for any customs officer "to go on board of any vessel, as well without as within his district, and to inspect, search, and examine the same, and any person, trunk, or envelope on board, and to this end, to hail and stop such vessel if under way, and to use all necessary force to compel compliance."[66] The customs officer had the authority to seize the items where it appeared "that any breach or violation of the laws of the United States [had] been committed" whereby "such vessel, or the goods, wares, and merchandise, or any part thereof, on board of or imported by such vessel, is or are liable to forfeiture."[67] This provision paralleled the fleeing-felon exception: the government did not need to first approach a third party magistrate for a warrant. The logic was that a crime was underway. In the latter context, it was the commission of a felony, and in the former context, the failure to pay duties at the border. Pari passu, the statute empowered officers to "arrest any person engaged in such breach or violation" and to pursue and arrest anyone

---

63. *See* An Act to provide more effectually for the collection of the duties imposed by law on goods, wares and merchandise imported into the United States, and on the tonnage of ships or vessels, ch. 35, §§ 48-51, 1 Stat. 145, 170 (1790); An Act for enrolling and licensing ships or vessels to be employed in the coasting trade and fisheries, and for regulating the same, ch. 8, § 27, 1 Stat. 305, 315 (1793); An Act altering the time of holding the District Court in Vermont, ch. 22, §§ 68-71, 1 Stat. 627, 677 (1799); *see also* An Act further to regulate the entry of merchandise imported into the United States from any adjacent territory, ch. 14, 3 Stat. 616 (1821); United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country.").

64. U.S. CONST. amend. IV.

65. An Act further to prevent Smuggling and for other Purposes, ch. 201, 14 Stat. 178 (1866).

66. *Id.* § 2.

67. *Id.*

who tried to escape.[68] Specifically, officers could stop, search, and examine "any vehicle, beast, or person on which or whom he . . . shall suspect there are goods, wares, or merchandise which are subject to duty or shall have been introduced into the United States in any matter contrary to law."[69] The statute reflected the importance of securing things to prevent the illegal movement of uncustomed goods—namely, the vehicle, animals, "goods, wares, or merchandise, and all other appurtenances, including trunks, envelopes, covers, and all means of concealment, and all the equipage, trappings, or other appurtenances of such beast."[70]

C. Contemporary Border Search Authorities

In 1930, the Smoot-Hawley Tariff Act increased tariffs on agricultural and industrial goods.[71] Eight years later, an amendment to the act provided for special inspection, examination, and search authorities.[72] As subsequently amended, the law empowers customs officers, acting pursuant to regulations issued by the Secretary of the Treasury or the Customs Service, to "enforce, cause inspection, examination, and search to be made of the persons, baggage, and merchandise discharged or unladen from" vessels arriving at U.S. ports, regardless of whether the goods have previously undergone inspection.[73]

In carrying out their duties, customs officers may board any vessel or vehicle "without as well as within [their] district[s]," in order 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."[74] Customs officers "may hail and stop such vessel or vehicle, and use all

---

68. *Id.*

69. *Id.* § 3.

70. *Id.*

71. Tariff Act of 1930, ch. 497, 46 Stat. 590 (codified as amended at 19 U.S.C. §§ 1301-1683g (2018)); *see also* Robert Whaples, *Where Is There Consensus Among American Economic Historians? The Results of a Survey on Forty Propositions*, 55 J. ECON. HIST. 139, 151 (1995) (finding consensus among economic historians that the Act "exacerbated the Great Depression").

72. Customs Administrative Act of 1938, ch. 679, 52 Stat. 1077, 1083 (codified as amended at 19 U.S.C. § 1467 (2018)).

73. 19 U.S.C. § 1467; *see also* 19 U.S.C. § 1496 ("The appropriate customs officer may cause an examination to be made of the baggage of any person arriving in the United States in order to ascertain what articles are contained therein and whether subject to duty, free of duty, or prohibited notwithstanding a declaration and entry therefor has been made."); 19 U.S.C. § 1499 (providing for entry examination of imported merchandise).

74. 19 U.S.C. § 1581(a).

necessary force to compel compliance."[75] The Treasury Secretary has the authority to issue regulations for searching persons and baggage.[76] Further, "all persons coming into the United States from foreign countries shall be liable to detention and search by authorized officers or agents of the Government under such regulations."[77]

As a matter of case law, the level of suspicion required to search travelers for illegal goods as they cross the border increases as the search becomes more intrusive. Courts, for instance, do not require particularized suspicion for the contents of a traveler's briefcase, luggage, purse, or pockets.[78] Nor is it required for documents within containers inside such items.[79] Pictures, films, and other graphic materials do not earn any higher level of protection.[80] Minimal suspicion is sufficient to warrant a pat-down.[81] In comparison, the search of a travelers' undergarments and strip searches require "real suspicion."[82] The only context thus far recognized by the Supreme Court as requiring individualized suspicion is related to the intimate physical search of a woman believed to be smuggling

---

75. *Id.*

76. *Id.* § 1582. The implementing regulations for the statutes can be found at 19 C.F.R. § 162.21 (2018).

77. 19 U.S.C. § 1582; *see also* Tariff Act of 1930, ch. 497, § 582, 46 Stat. 590, 748 (enacting § 1582).

78. *See, e.g.*, United States v. Tsai, 282 F.3d 690, 696 (9th Cir. 2002); Henderson v. United States, 390 F.2d 805, 808 (9th Cir. 1967). But note that suspicion as a basis for detention and questioning cannot be based merely on ancestry. *See* United States v. Brignoni-Ponce, 422 U.S. 873, 886-87 (1975).

79. *See* United States v. Grayson, 597 F.2d 1225, 1228-29 (9th Cir. 1979).

80. *Cf.* United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971) (holding that the seizure of obscene photographs at a port of entry was not unconstitutional, for "[c]ustoms officers characteristically inspect luggage and their power to do so is not questioned in this case; it is an old practice and is intimately associated with excluding illegal articles from the country").

81. Guam v. Sugiyama, 846 F.2d 570, 572 (9th Cir. 1988) (finding a pat-down to be appropriate when the suspect was known to be connected to packages of marijuana previously sent to the airport); *accord* United States v. Des Jardins, 747 F.2d 499, 504-05 (9th Cir. 1984), *vacated in part*, 772 F.2d 578 (9th Cir. 1985) (finding a pat-down was justified when objects frequently used in narcotics smuggling were found in the traveler's suitcase); United States v. Quintero-Castro, 705 F.2d 1099, 1100-01 (9th Cir. 1983) (finding a pat-down to be appropriate where the traveler paid cash for the ticket, appeared nervous, and the traveler's story conflicted with a co-traveler's story); United States v. Carter, 563 F.2d 1360, 1360-61 (9th Cir. 1977) (finding a pat-down to be appropriate when the traveler appeared nervous and did not directly answer questions about the trip); United States v. Rivera-Marquez, 519 F.2d 1227, 1228 (9th Cir. 1975) (finding a pat-down to be appropriate when an informant told agents that an individual with the traveler's name would be smuggling drugs on that day).

82. *Des Jardins*, 747 F.2d at 505; United States v. Couch, 688 F.2d 599, 604 (9th Cir. 1982); United States v. Guadalupe-Garza, 421 F.2d 876, 879 (9th Cir. 1970).

drugs in her alimentary canal.[83] In the 1985 case *United States v. Montoya de Hernandez*, customs officials suspected that a woman had swallowed balloons containing drugs.[84] The Supreme Court determined that reasonable suspicion was required to detain the individual until the drugs had passed.[85] This decision followed a series of lower court cases rejecting mere suspicion for intrusive body searches, requiring a "clear indication" or "plain suggestion" of criminal activity.[86]

Vehicle searches are subject to a less rigorous standard than are searches of persons. In *United States v. Flores-Montano*, reasonable suspicion was not considered necessary for removing a gas tank to search for contraband.[87] The Supreme Court, however, has held open the possibility "that some searches of *property* are so destructive as to require" particularized suspicion.[88]

D. Mail Search

The discussion above addresses goods and materials crossing U.S. borders. Special laws address the search of items sent through the postal system, where stronger protections are afforded to citizens' communications. These measures sharply contrast with the lack of restrictions over CBP's current search of electronic mail—the modern-day equivalent of the post.

---

83. United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985).

84. *Id.* at 534.

85. *Id.* at 541.

86. *See, e.g.*, United States v. Vance, 62 F.3d 1152 (9th Cir. 1995) (holding "real suspicion" was present when the defendant, traveling from Hawaii to Guam, underwent a pat-down search). In *Vance*, a customs officer observed that the traveler was glassy-eyed, disoriented, and had trouble answering questions. A pat-down revealed two pairs of underwear and a bulge at the traveler's crotch. When directed to drop his underwear, two packs of methamphetamine fell out. *Montoya de Hernandez* rejected the Ninth Circuit's use of the "clear indication" language as an intermediate standard between "reasonable suspicion" and "probable cause" and established that "clear indication" stood for "the necessity for particularized suspicion that the evidence sought might be found within the body of the individual." 742 U.S. at 540.

87. 541 U.S. 149, 150, 155 (2004). In this case, the Ninth Circuit had taken the term "routine" from *Montoya de Hernandez*, created a balancing test, and applied it to vehicle searches. *Id.* at 152. The Supreme Court objected, determining that searches of vehicles were subject to a much less rigorous standard than searches of a person. *Id*. The Ninth Circuit went on in *United States v. Chaudhry*, 424 F.3d 1051, 1054 (9th Cir. 2005), to find the distinction between "routine" and "non-routine" inapplicable to searches of property.

88. United States v. Flores-Montano, 541 U.S. 149, 155-56 (2004) (emphasis added) (holding that complete disassembly and reassembly of a car gas tank did not require particularized suspicion).

In regard to traditional communications, customs officers do not have the authority to open and inspect mail weighing sixteen ounces or less.[89] They may only read correspondence contained in mail sealed against inspection once they have obtained either (a) written consent by the sender or addressee or (b) a search warrant from a judicial officer that meets the requirements of Rule 41 of the Federal Rules of Criminal Procedure.[90] These restrictions do not apply to mail that has not been sealed against inspection.[91] The key difference is the sealing of the document.

Mail weighing more than sixteen ounces that has been sealed against inspection can only be opened and searched by a customs officer where there are reasonable grounds to suspect that it contains (a) monetary instruments, (b) a weapon of mass destruction, or (c) material related to one of six categories.[92] These include: exportation or importation of monetary instruments;[93] material related to obscenity or child pornography;[94] controlled substances;[95] nuclear materials covered by the Export Administration Act;[96] defense articles and services;[97] and emergency matters that fall within the International Emergency Economic Powers Act, such as foreign exchange, transfers of credit or payments, or the import or export of currency or securities.[98]

A different provision in the code, the origins of which stem from nineteenth-century statutes, deals specifically with opening trunks or envelopes on board vessels.[99] The standard set is "reasonable cause." The statute authorizes customs offers boarding vessels to "search any trunk or envelope, wherever found, in which he may have a reasonable cause to suspect there is merchandise which was

89. 19 U.S.C. § 1583(d) (2018).

90. *Id.* § 1583(c)(2).

91. *Id.* § 1583(b).

92. *Id.* § 1583(c)(1).

93. *Id.* § 1583(c)(1)(A); *see also* 31 U.S.C. § 5316 (2018) (requiring the reporting of the export and import of certain monetary instruments).

94. 19 U.S.C. § 1583(c)(1)(F); *see also* 18 U.S.C. §§ 1461, 1463, 1465, 1466 (2018) (prohibiting the interstate sale and transmission of obscene materials).

95. 19 U.S.C. § 1583(c)(1)(D); *see also* 21 U.S.C. § 953 (2018) (listing controlled substances that are unlawful to export and certain exceptions to said default prohibition).

96. 19 U.S.C. § 1583(c)(1)(G); *see also* 50 U.S.C. app. §§ 2403, 2404, 2415 (2018) (granting the President authority to control the export of goods and technology related to nuclear materials).

97. 22 U.S.C. § 2778 (2018).

98. 50 U.S.C. §§ 1701-1702 (2018).

99. 19 U.S.C. § 482 (recodified by Rev. Stat. § 3061, which derived from the Act of July 18, 1866, ch. 201 § 3, 14 Stat. 178, 178).

imported contrary to law.[100] The Court has upheld the reasonable-suspicion test as applied to border searches as constitutional.[101]

E. Extended Border Search and the Functional Equivalent

For searches away from ports of entry, courts look at whether such actions can be upheld as "extended border searches" (i.e., searches proximate to the border) as well as whether they take place at the "functional equivalent" of the border (i.e., a place that may be far from the physical border, but which acts as border crossing). [102] Airports, for instance, are considered the functional equivalent of the border.[103] The validity of such searches depends upon a variety of factors, suggesting a totality-of-circumstances test. As with searches at the actual border, the Fourth Amendment standard of "reasonableness" still applies; however, mere suspicion is sufficient.[104]

In cases of continuous surveillance of vehicles transiting the border, courts have upheld searches twenty miles from the border that occur fifteen hours after entry.[105] On the other hand, for roving searches, the Supreme Court has held

---

100. *Id.*

101. *Id.*

102. Torres v. Puerto Rico, 442 U.S. 465 (1979) (holding that the search of an individual arriving in the Commonwealth of Puerto Rico from the United States did not satisfy Fourth Amendment requirements because the individual did not cross the functional equivalent of an international border of the United States); United States v. Carter, 760 F.2d 1568 (11th Cir. 1985).

103. Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973) ("For . . . example, a search of the passengers and cargo of an airplane arriving at a St. Louis airport after a nonstop flight from Mexico City would clearly be the functional equivalent of a border search.").

104. Alexander v. United States, 362 F.2d 379 (9th Cir. 1966) (citing Cervantes v. United States, 263 F.2d 800, 803 n.5 (9th Cir. 1959)); *see also* Carroll v. United States, 267 U.S. 132, 154, (1925); Boyd v. United States, 116 U.S. 616, 623, (1886); Hammond v. United States, 356 F.2d 931 (9th Cir. 1966); King v. United States, 348 F.2d 814, 817 (9th Cir. 1965); Jones v. United States, 326 F.2d 124, 130 (9th Cir. 1964) (Duniway, J., concurring); Denton v. United States, 310 F.2d 129 (9th Cir. 1962); Mansfield v. United States, 308 F.2d 221 (5th Cir. 1962); Plazola v. United States, 291 F.2d 56 (9th Cir. 1961); Witt v. United States, 287 F.2d 389 (9th Cir. 1961); Murgia v. United States, 285 F.2d 14 (9th Cir. 1960); Landau v. U.S. Att'y, 82 F.2d 285 (2nd Cir. 1936); United States v. Wischerth, 68 F.2d 161 (2d Cir. 1933); United States v. Yee Ngee How, 105 F. Supp. 517 (N.D. Cal. 1952).

105. *See, e.g.*, Bloomer v. United States 409 F.2d 869 (9th Cir. 1969) (upholding s search in which an Oldsmobile with marijuana was under constant surveillance from the time it crossed the border); Rodriguez-Gonzalez v. United States, 378 F.2d 256 (9th Cir. 1967) (holding that mere suspicion is acceptable for a search that took place fifteen hours after entry and twenty miles from the border and that found marijuana hidden in a rear door because the search met the totality-of-the-circumstances test—time and distance, extent, and manner); Gonzalez-Alonso v. United States, 379 F.2d 347 (9th Cir. 1967) (holding valid, after applying the totality-of-the-circumstances test, a search that found marijuana in a car after following it eleven

invalid a warrantless search, twenty-five miles north of the border, on an east-west highway located at all points at least twenty miles from border, absent probable cause and reasonable suspicion.[106] There is no border exception outside the actual border or its functional equivalent.[107]

F. Special Protections Afforded to the Home

As the Supreme Court noted in 1977, "a port of entry is not a traveler's home."[108] For centuries, the courts have applied special protections to the latter. From the time of Coke's *Institutes* (and, arguably, the Magna Carta), except in instances of a fleeing felon or the hue and cry, common law forbade access to the home absent a particularized warrant.[109] The need for such a document increased pressure on what, precisely, would satisfy the requirement.

In the seventeenth and eighteenth centuries, the Crown began to make use of general warrants: documents issued by the monarch or a judicial officer, which

---

miles inland); Lee v. United States, 376 F.2d 98 (9th Cir. 1967), *cert. denied*, 389 U.S. 837 (holding that the actions of a customs agent who placed a car from Mexico under surveillance following a tip and later found narcotics in the car and arrested its occupants were legal because the car was continuously under surveillance); Leeks v. United States, 356 F.2d 470 (9th Cir. 1966) (upholding a search fifteen miles north of the San Ysidro border entry after customs officers' continuous tailing); Alexander v. United States, 362 F.2d 379 (9th Cir. 1966), *cert. denied*, 385 U.S. 977 (upholding a search in which heroin was discovered after agents placed a vehicle crossing into Arizona under surveillance, reasoning that by statute customs officers had long had the express authority to stop, search, and examine vehicles suspected of carrying merchandise subject to duty, making it possible for them to do what would be "unreasonable" for police as long as the totality of the circumstances could convince a factfinder with reasonable certainty); King v. United States, 348 F.2d 814 (9th Cir. 1965), *cert. denied*, 382 U.S. 926 (upholding a search by a customs agent who, based on a tip, followed a car at a crossing near Tijuana).

106. *See Almeida-Sanchez*, 413 U.S. at 266. In *Almeida-Sanchez*, a Mexican citizen with a valid U.S. work permit was convicted for possession and transfer of marijuana following a warrantless search of his automobile. *Id.* at 267. The government argued that the Immigration and Nationality Act, which provided for warrantless searches "within a reasonable distance [defined by regulations as 100 air miles] from any external boundary" authorized the search. Immigration and Nationality Act § 287(a)(3), 8 U.S.C. § 1357(a) (2018); *see also* 8 C.F.R. § 287.1 (2018). In a 5-4 opinion, the Supreme Court ruled that the statute and regulation, which permitted searches within 100 miles of the border, were inconsistent with the Fourth Amendment. The Court also held that the search could not be justified on the basis of the rules applied to a search of automobiles. In *Carroll v. United States*, the Court upheld a clause in the Volstead Act that allowed for warrantless searches of automobiles where probable cause existed. 267 U.S. 132 (1925). In this case, however, agents had not met the standard of probable cause.

107. United States v. Ortiz, 422 U.S. 891 (1975).

108. United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971).

109. Donohue, *supra* note 19, at 1207-12.

were not based on any prior evidence of wrongdoing. Instead, general warrants were used to *find* criminal activity. They lacked particularity regarding the person or place to be searched, or the papers or records to be seized. They were not supported by oath or affirmation. The risk was that such nonparticularized warrants could be used to target individuals opposed to the Crown, and to find some reason (or excuse) to subject them to legal process. Treatise writers and jurists roundly condemned the practice as unreasonable—in other words, against the reason of the common law.[110] Only specific warrants, issued by a magistrate, naming the individual, establishing probable cause for a specific crime, and supported by oath or affirmation, met the standard.[111] The Framers incorporated this common law rule into the Fourth Amendment.[112]

Even with a warrant, there were strict limits on what could be sought. Particularized warrants only permitted officers to search for the fruits and instrumentalities of a crime. They could not look for "mere evidence." This rule did not fall out of favor until 1967, just a few months prior to the Supreme Court's decision in *Katz v. United States*.[113]

As a matter of customs law, from the beginning, Congress and the courts drew a distinction between a store or dwelling house, or other structure for which a proper warrant was required, and the search of a ship, motorboat, wagon, or automobile, where it was not practicable to obtain a warrant because the vehicle could be quickly moved. Thus, under the Act of March 3, 1815, it was not only lawful to board and search vessels within the customs officers' districts and those adjoining, but also to stop and search any vehicle, beast, or person for

110. *Id.* at 1269-76.

111. *Id.* at 1235-40.

112. U.S. CONST. amend. IV; *see also* Donohue, *supra* note 19, at 1298-1305.

113. *See* Warden, Md. Penitentiary v. Hayden, 387 U.S. 294 (1967); Schmerber v. California, 384 U.S. 757 (1966); *see also* Katz v. United States, 389 U.S. 347 (1967). In constructing the mere evidence rule, the Court drew a distinction between the fruits and instrumentalities of crime, on the one hand, and other types of materials. In *Boyd v. United States*, Justice Bradley, writing for the Court, explained: "The search for and seizure of stolen or forfeited goods . . . are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him." 116 U.S. 616, 623 (1886). For the Court, the two things differed "*toto coelo*," (completely) because "[i]n the one case, the government is entitled to the possession of the property; in the other it is not." *Id.* From the beginning, no one expected the Fourth Amendment warrant requirement to apply to contraband or uncustomed goods at the border. *Id.* at 623-24. Even as the Court dispensed with the mere evidence rule, in doing so, it agonized that this move would be taken as an invitation to pry into the privacies of life. In a post-*Katz* world, the test applied would be not just one of property, but of an objective and subjective expectation of privacy. For a critique of this standard, see generally Laura K. Donohue, *Functional Equivalence and Residual Rights Post-Carpenter: Framing a Test Consistent with Precedent and Original Meaning*, 2019 SUP. CT. REV. (forthcoming).

whom there was probable cause to believe unlawful goods had been brought into the United States.[114] The Court considered it a valid exercise of constitutional power.[115] To the extent that a question of distance from the border arose, in the nineteenth century, the Attorney General drew the line at three miles.[116]

In this way, the border exception also bore a striking resemblance to the fleeing felon exception: it was only in the hot pursuit of goods illegally brought into the country that broader powers could be exercised. Limits still applied. "It would be intolerable and unreasonable," the Court explained, "if a prohibition agent were authorized to stop every automobile on the chance of finding liquor, and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search."[117] As the Court wrote in *Carroll v. United States*:

> Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in. But those lawfully within the country, entitled to use the public highways, have a right to free passage without interruption or search unless there is known to a competent official, authorized to search, probable cause for believing that their vehicles are carrying contraband or illegal merchandise.[118]

---

114. Act of Mar. 3, 1815, ch. 94, 3 Stat. 231, 232. For total or partial renewals of the statute, see Act of Apr. 27, 1816, ch. 110, 3 Stat. 315; Act of Feb. 28, 1865, ch. 67, 13 Stat. 441; Act of July 18, 1866, ch. 201, 14 Stat. 178; Rev. Stat. § 3061.

115. Cotzhausen v. Nazro, 107 U.S. 215 (1883); *see also* United States v. One Black Horse, 129 F. 167 (D. Me. 1904). Similar provisions applied to Indian agents who, suspecting the introduction of alcohol, could cause the boats, stores, packages, wagons, sleds, and places of deposit to be searched and seized. Rev. Stat. § 2140 (1875). This power arose from an 1822 statute that allowed for traders' goods to be searched and seized on basis of suspicion of alcohol, *see* Act of May 6, 1822, ch. 58, 3 Stat. 682), as well as the Act of June 30, 1834, § 20, ch. 161, 4 Stat. 729, 732. The Supreme Court recognized the Statute of 1822 as sufficient for search and seizure in *American Fur Co. v. United States*, 27 U.S. (2 Pet.) 358, 366-67 (1829). All of these statutes are cited and discussed in *Carroll v. United States*, 267 U.S. 132 (1925).

116. Act of Mar. 3, 1899, ch. 429, § 174, 30 Stat. 1253, 1280. The Attorney General, construing the Act, wrote, "If your agents reasonably suspect that a violation of law has occurred, in my opinion they have power to search any vessel within the three-mile limit according to the practice of customs officers when acting under section 3059 of the Revised Statutes [Comp. St. § 5761], and to seize such vessels." Auth. of Agents of the Dep't of Commerce & Labor to Make Arrests, 26 Op. Att'y Gen. 243, 246 (1907). This language is cited and quoted in *Carroll*, 267 U.S. at 153.

117. *Carroll*, 267 U.S. at 153-54.

118. *Id.* at 154.

In *Carroll*, the Court noted the necessity of establishing probable cause of a felony for a search that occurred away from the border. The border was only relevant insofar as it helped to establish probable cause.[119]

Reflecting these traditions, customs searches of homes currently require a warrant, issued by a third-party federal judge or magistrate, and supported by probable cause that merchandise has been illegally brought into the United States, or that the goods in question are subject to forfeiture.[120] The search of vehicles or vessels, however, is not limited to the time and place of actual international crossings.[121]

G. Restrictions on Customs Searches: Who and Why

Even when the customs exception applies, not every government official is permitted to exercise the associated enforcement powers. Courts have held that an "officer of the customs" includes customs officers, inspectors, investigators, and mail entry aides, certain Immigration and Naturalization Service officials (such as border patrol agents), and Coast Guard officers.[122] The term also includes a doctor aiding a customs search.[123] The right to undertake border searches does *not* extend to the FBI or to law enforcement when acting for general law enforcement purposes.

In the 1979 case of *United States v. Vidal Soto-Soto*, for example, the Ninth Circuit considered the FBI's warrantless search of a Chevrolet pickup truck at the border to determine whether it had been stolen.[124] The agent's sole basis for stopping the truck was the make and model of the vehicle.[125] Instead of

---

119. *Id.* at 160.

120. 19 U.S.C. § 1595 (2018).

121. 19 U.S.C. § 482 ("Any of the officers or persons authorized to board or search vessels may stop, search, and examine, as well without as within their respective districts, any vehicle, beast, or person, on which or whom he or they shall suspect there is merchandise which is subject to duty, or shall have been introduced into the United States in any manner contrary to law . . . and to search any trunk or envelope, wherever found, in which he may have a reasonable cause to suspect there is merchandise which was imported contrary to law."). This section dates back to Act of Mar. 3, 1815, ch. 94, 3 Stat. 231, 232; Act of July 18, 1866, ch. 201, 14 Stat. 178.

122. *See Who May Conduct Border Search Pursuant to 19 U.S.C.A. § 482, 1401(i), 1581 (a,b), and 1582*, 61 A.L.R. Fed. 290, at §§ 3, 4; *see also* 19 U.S.C. § 1401(i) (defining "customs officer" to mean "any commissioned, warrant, or petty officer of the Coast Guard, or any agent or other person, including foreign law enforcement officers, authorized by law or designated by the Secretary of the Treasury to perform any duties of an officer of the Customs Service.").

123. *Id.*

124. United States v. Vidal Soto-Soto, 598 F.2d 545, 546 (9th Cir. 1979).

125. *Id.*

evaluating the case under the customs search exception, the court instead looked to the Supreme Court's recent decision in *Delaware v. Prouse*, in which it had required articulable and reasonable suspicion that a motorist was unlicensed or an automobile not registered to detain a vehicle and request the registration papers.[126]

The broader search authority granted to customs officers is based on the need to interdict things illegally brought into the country. As the Ninth Circuit noted, "[v]alidity for this distinction is found in the fact that the primordial purpose of a search by customs officers is not to apprehend persons, but to seize contraband property unlawfully imported or brought into the United States."[127] The court observed that "[t]he authorization of section 581 [19 U.S.C. § 1581] is to ascertain whether there are any dutiable articles concealed in the vessel; it is not to discover acts of criminality."[128] The purpose is "to effectuate the provisions of the navigation and tariff laws and to protect the revenue of the United States."[129] It is not to deter criminal activity writ large.[130]

III. IMMIGRATION BORDER SEARCH AUTHORITIES

Immigration law has followed a different trajectory from provisions related to uncustomed goods and contraband. The doctrine is fraught with contradictions regarding the constitutional power of federal versus state entities.[131] At the same time, history demonstrates that the primary aim of federal immigration inspection has been (a) to establish travelers' identity; (b) to ensure that travelers meet the requirements for legal entry; and (c) to collect money to fund immigration services. An additional immigration interest—namely, keeping convicted criminals out of the country—only applies to non-citizens. This aim sheds light on some of the differences between CBP and ICE regulations.

---

126. Delaware v. Prouse, 440 U.S. 648 (1979).

127. Alexander v. United States, 362 F.2d 379, 382 (1966); *see also* Olson v. United States, 68 F.2d 8 (2d Cir. 1933) (finding that a "search of a vessel by officers of the Coast Guard or of the customs for the purpose of discovering a cargo which might be subject to duty should not be regarded as unreasonable even though the search, as distinguished from the seizure, is made without probable cause").

128. *Olson*, 68 F.2d at 9.

129. *Id.* at 10.

130. But note that seizure may rest on a violation of criminal law. *See* Maul v. United States, 274 U.S. 501 (1927); Wood v. United States, 41 U.S. 342 (1842); Awalt v. United States, 47 F.2d 477 (3d Cir. 1931).

131. *See* Hiroshi Motomura, *Immigration Law After a Century of Plenary Power: Phantom Constitutional Norms and Statutory Interpretation*, 100 YALE L.J. 545 (1990).

In 1790, pursuant to Article I, Section 8 of the Constitution, Congress introduced rules for naturalization; however, it did not institute any restrictions on immigration.[132] Through the late nineteenth century, immigration to the United States was thus relatively unregulated.[133] In 1875, Congress passed the first federal immigration law.[134] That statute entrusted the inspection of immigrants to customs collectors at the ports of entry. It excluded criminals and prostitutes and prohibited human trafficking of individuals from Asia.[135] The inspectors had to ensure that these statutory requirements were met, which could only be done at the point of arrival. That same year, the Supreme Court ruled that immigration was a matter reserved to the federal government.[136]

In *Chy Lung v. Freeman*, the Court considered a California law that had extended significant powers of inspection, the ability to charge for every examination, and the ability to set a bond for each passenger, to the state Commissioner of Immigration.[137] Justice Miller, writing for the Court, observed: "The passage of laws which concern the admission of citizens and subjects of foreign nations to our shores belongs to Congress, and not to the States."[138] Congress's dominion over international commerce and its ability to shape U.S. foreign affairs were tied to its ability to regulate immigration.[139]

---

132. U.S. CONST. art. I, § 8, cl. 4 (authorizing Congress "[t]o establish a uniform rule of naturalization"); An Act to establish an uniform Rule of Naturalization, ch. 3, 1 Stat. 103 (1790).

133. *Overview of INS History*, U.S. CITIZENSHIP & IMMIGR. SERVS. (2012) [hereinafter USCIS Report], https://www.uscis.gov/sites/default/files/USCIS/History%20and%20Genealogy/Our%20History/INS%20History/INSHistory.pdf [https://perma.cc/ZQ5V-AA5Z]. Following the Civil War, some states introduced immigration laws. *Id.* at 3.

134. Page Act of 1875, ch. 141, 18 Stat. 477.

135. *Id.*

136. Chy Lung v. Freeman, 92 U.S. 275, 280 (1875).

137. *See id.* at 277-78; 1 THEODORE H. HITTEL, CODES AND STATUTES OF THE STATE OF CALIFORNIA 364-69 (1876) (giving the Commissioner of Immigration the power "to satisfy himself whether or not any passenger who shall arrive in this state by vessels from any foreign port or place (who is not a citizen of the United States), is lunatic, idiotic, deaf, dumb, blind, crippled or infirm, and is not accompanied by relatives who are able and willing to support him, or is likely to become permanently a public charge, or has been a pauper in any other country, or is, from sickness or disease . . . a public charge, or likely soon to become so, or is a convicted criminal, or a lewd or debauched woman"). The Court objected: "It is hardly possible to conceive a statute more skillfully framed, to place in the hands of a single man the power to prevent entirely vessels engaged in a foreign trade . . . from carrying passengers, or to compel them to submit to systematic extortion of the grossest kind." *Chy Lung*, 92 U.S. at 278.

138. *Id.* at 280.

139. *Id.* ("It has the power to regulate commerce with foreign nations: the responsibility for the character of those regulations, and for the manner of their execution, belongs solely to the national government. If it be otherwise, a single State can, at her pleasure, embroil us in disastrous quarrels with other nations.").

Fifteen years later, in *Chae Chan Ping v. United States*, the Court stated that although the Constitution did not explicitly address immigration, Congress had the general power to pass a statute amending prior treaties and excluding Chinese citizens.[140] Justice Field, writing for the Court, said, "[t]he question whether our government is justified in disregarding its engagements with another nation is not one for the determination of the courts."[141] The decision fell to the political branches, rendering any judicial "reflection upon [Congress's] motives, or the motives of any of its members," immaterial.[142] The Court wrote:

> That the government of the United States, through the action of the legislative department, can exclude aliens from its territory is a proposition which we do not think open to controversy. Jurisdiction over its own territory to that extent is an incident of every independent nation. It is a part of its independence. If it could not exclude aliens it would be to that extent subject to the control of another power.[143]

Such authority was part of the foreign affairs power of any country, found in the interstices of Article I, Section 8, and Article II.[144]

With the authority to pass immigration laws firmly in federal hands, Congress passed a series of statutes providing for powers of inspection. Some laws, particularly those related to Chinese exclusion and contract labor, focused on establishing the identity of travelers.[145] Under the Chinese Exclusion Act of 1882, for instance, the collector of customs in the district from which Chinese laborers departed from the United States were empowered to "go on board each vessel" and "make a list" of all Chinese laborers, entering the information into registry books with details on each worker's "name, age, occupation, last place of residence, physical marks or peculiarities, and all facts necessary

---

140. Chae Chan Ping v. United States, 130 U.S. 581 (1888); Chinese Exclusion Act of 1882, ch. 126, 22 Stat. 58 ("execut[ing] certain treaty stipulations relating to Chinese").

141. *Chae Chan Ping*, 130 U.S. at 602.

142. *Id.* (citing Taylor v. Morton, 23 F. Cas. 784 (C.C.D. Mass. 1855) (No. 13,799), *aff'd*, 67 U.S. 481 (1862)).

143. *Id.* at 603-04.

144. *Id.* at 604 ("The powers to declare war, make treaties, suppress insurrection, repel invasion, regulate foreign commerce, secure republican governments to the States, and admit subjects of other nations to citizenship, are all sovereign powers, restricted in their exercise only by the Constitution itself and considerations of public policy and justice which control, more or less, the conduct of all civilized nations.").

145. *See, e.g.*, Alien Contract Labor Law of 1885, ch. 164, 23 Stat. 332 (prohibiting "the importation and migration of foreigners and aliens under contract or agreement to perform labor in the United States"); Alien Contract Labor Law of 1887, ch. 220, 24 Stat. 414; Alien Contract Labor Law of 1888, ch. 1210, 25 Stat. 566 (authorizing the Secretary of Treasury to cause immigrants landing contrary to prohibitions to be returned within one year of landing).

for . . . identification."[146] The same year, Congress passed another law that established a system of central control and created new classes of aliens that would be inadmissible to the United States based on whether they were likely to become a public burden or exhibited dubious moral character.[147] Measures also addressed revenue generation, which gave inspectors further powers at the ports of entry.[148]

In 1891, Congress passed its first comprehensive immigration law, creating a Bureau of Immigration within the Treasury Department to administer all immigration laws (except the Chinese Exclusion Act), and further restricted immigration by adding inadmissible classes of persons, empowering the Secretary of Treasury to issue rules for inspection along the Canadian border, and directing the deportation of illegal aliens.[149] In 1893, Congress augmented the reporting requirements to include travelers' occupation, marital status, literacy, money in possession, and physical as well as mental health.[150] A decade later, Congress expanded the list to provide for the exclusion of aliens based on political views—including "anarchists, or persons who believe in, or advocate, the overthrow by force or violence the government of the United States, or of all government, or of all forms of law, or the assassination of public officials."[151] In 1907, Congress expanded exclusion to cover "imbeciles", "feeble-minded

---

146. Chinese Exclusion Act of 1882, ch. 126, § 4, 22 Stat. 58; *see also id.* § 1 (suspending entry of Chinese laborers for 10 years); *id.* § 3 (requiring that evidence of residence prior to passage of the Act be presented to the master of the vessel and the collector of the port); *id.* § 8 (requiring the master of any vessels arriving in the United States to provide details of any Chinese passengers on board); *id.* § 9 (empowering the collector "to examine such passengers, comparing the certificates with the list and with the passengers").

147. Immigration Act of 1882, ch. 376, § 4, 22 Stat. 214 (excluding convicts, except those convicted of political offenses, from entry).

148. *See, e.g.*, *id.* § 1 (establishing a duty for every passenger arriving in the United States); *id.* § 3 (giving the Secretary of the Treasury the authority to establish regulations to protect the United States from fraud and loss); Immigration Act of 1917, ch. 29, § 2, 39 Stat. 874, 875 (establishing a tax of eight dollars for every alien, with certain exceptions and establishing for its collection by the collector of customs of the port in which the alien arrives).

149. Alien Contract Law of 1891, ch. 551, § 1, 26 Stat. 1084 (excluding certain classes of aliens "in accordance with the existing acts regulating immigration," namely: "[a]ll idiots, insane persons, paupers or persons likely to become a public charge, persons suffering from a loathsome or a dangerous contagious disease, persons who have been convicted of a felony or other infamous crime or misdemeanor involving moral turpitude, polygamists, and also any person whose ticket is paid for with the money of another or who is assisted by others to come, unless it is affirmatively and satisfactorily shown on special inquiry that such person does not belong to one of the foregoing excluded classes," or to the contract laborers excluded by the 1885 statute).

150. Act of Mar. 3, 1893, ch. 206, 27 Stat. 569.

151. Immigration Act of Mar. 3, 1903, ch. 1012, 32 Stat. 1213.

persons", persons with physical or mental defects, persons afflicted with tuberculosis, children unaccompanied by their parents, persons who admitted the commission of a crime involving moral turpitude, and women entering the country for immoral purposes.[152] Just as certain classes of people were excluded, others were encouraged to enter, including artists, singers, ministers, professors, and domestic servants. Immigration officials had the power to make inquiries necessary for these determinations.

In 1907, Congress established a Joint Commission on Immigration to consider the entire system and ten years later implemented the Commission's recommendations.[153] The 1917 statute added new excludable classes and a literacy test, and created the Asiatic Barred Zone, which encompassed much of the Asian continent.[154] During World War I, Congress further passed a measure to give the President broad power to control the entry and exit of aliens in the interests of public safety.[155]

For the balance of the twentieth century, immigration measures focused on defining admissible aliens.[156] These statutes, without exception, focused on

---

152. Immigration Act of Feb. 20, 1907, ch. 1134, 34 Stat. 898.

153. *Id.*; Immigration Act of Feb. 5, 1917, 39 Stat. 874; An Act to Amend Section 23 of the Immigration Act of Feb. 5, 1917, 39 Stat. 874.

154. Immigration Act of Feb. 5, 1917, 39 Stat. 874, § 3 (excluding "[a]ll idiots, imbeciles, feebleminded persons, epileptics, insane persons; persons who have had one or more attacks of insanity at any time previously; persons of constitutional psychopathic inferiority; persons with chronic alcoholism; paupers; professional beggars; vagrants; persons afflicted with tuberculosis in any form or with a loathsome or dangerous contagious disease; persons not comprehended within any of the foregoing excluded classes who are found to be and are certified by the examining surgeon as being mentally or physically defective, such physical defect being of a nature which may affect the ability of such alien to earn a living; persons who have been convicted of or admit having admitted a felony or other crime or misdemeanor involving moral turpitude; polygamists, or persons who practice polygamy or believe in or advocate the practice of polygamy; anarchists, or persons who believe in or advocate the overthrow by force or violence of the Government of the United States, or of all forms of law, or who disbelieve in or are opposed to organized government, or who advocate the assassination of public officials, or who advocate or teach the unlawful destruction of property; persons who are members of or affiliated with any organization entertaining and teaching disbelief in or opposition to organized government, or who advocate or teach the duty, necessity, or propriety of the unlawful assaulting or killing of any officer or officers, either of specific individuals or of officers generally, of the Government of the United States or of any other organized government . . . prostitutes, or persons coming into the United States for the purpose of prostitution or for any other immoral purpose . . . contract laborers . . . all children under sixteen years of age, unaccompanied by . . . their parents" and individuals from parts of the Asian Continent).

155. Act of May 22, 1918, Pub. L. No. 65-154, 40 Stat. 559.

156. *See, e.g.*, Act of May 19, 1921, Pub. L. No. 67-5, 42 Stat. 5 (setting the first quota for aliens entering the United States); Act of May 11, 1922, Pub. L. No. 67-55, 42 Stat. 540 (extending

and amending the Act of May 19, 1921); Immigration Act of 1924, Pub. L. No. 68-139, 43 Stat. 153 (establishing the first permanent limitation on immigration—the "national origins quota system," which remained in place until the Immigration and Nationality Act of 1952); Joint Resolution of Mar. 31, 1928, Pub. Res. No. 70-20, 45 Stat. 400 (postponing introduction of quotas until July 1929); Act of Apr. 2, 1928, Pub. L. No. 70-234, 45 Stat. 401 (excluding American Indians born in Canada from application of the Immigration Act of 1924); Act of Mar. 2, 1929, Pub. L. No. 70-962, 45 Stat. 1512 (establishing record of prior lawful admission; subsequently folded into the Alien Registration Act of 1940); Act of Mar. 17, 1932, Pub. L. No. 72-61, 47 Stat. 67 (applying the contract labor provisions of the immigration laws to instrumental musicians); Act of May 2, 1932, Pub. L. No. 72-115, 47 Stat. 145 (doubling allocation for the enforcement of the contract labor provisions of the immigration laws); Act of July 1, 1932, Pub. L. No. 72-234, 47 Stat. 524 (providing for specified classes of nonimmigrant aliens to be admitted for a prescribed amount of time); Act of July 11, 1932, Pub. L. No. 72-277, 47 Stat. 656 (providing non-quota status to the husbands of American citizens, as wives were already accorded non-quota status); Alien Registration Act, 1940, Pub. L. No. 76-670, 54 Stat. 670 (requiring alien registration and making membership in proscribed organizations grounds for exclusion); Act of June 20, 1941, Pub. L. No. 77-113, 55 Stat. 252 (allowing consular officers to refuse a visa to anyone believed to be seeking entry for purposes of engaging in activities that would endanger the safety of the United States); Act of June 21, 1941, Pub. L. No. 77-114, 55 Stat. 252 (extending the Act of May 22, 1918 and giving the President the power, during national emergency or war, to prevent aliens from entering the United States); Act of Apr. 29, 1943, Pub. L. No. 78-45, 57 Stat. 70 (providing for the importation of temporary agricultural laborers to the United States from the Americas, to help in agriculture during World War II); Act of Dec. 17, 1943, Pub. L. No. 78-199, 57 Stat. 600 (amending the Alien Registration Act of 1940 and adding Chinese persons to the class of aliens eligible for naturalization); Act of Feb. 14, 1944, Pub. L. No. 78-229, 58 Stat. 11 (providing for the importation of temporary workers from the Western Hemisphere); Act of June 29, 1946, Pub. L. No. 79-471, 60 Stat. 339 (facilitating U.S. armed force members' fiancées admission to the United States); Act of July 2, 1946, Pub. L. No. 79-483, 60 Stat. 416 (amending the Immigration Act of 1917 and giving persons of races indigenous to India and Filipino descent admission to the United States); Act of May 25, 1948, Pub. L. No. 80-552, 62 Stat. 268 (excluding anarchists and similar classes); Displaced Persons Act of 1948, Pub. L. No. 80-774, 62 Stat. 1009 (permitting the first formal admission of persons fleeing persecution, subject to a quota); Central Intelligence Agency Act of 1949, Pub. L. No. 81-110, 63 Stat. 208 (authorizing the admission of up to 100 people by the CIA annually, where in the interests of national security); Act of June 30, 1950, Pub. L. No. 81-857, 64 Stat. 306 (providing for up to 250 skilled sheepherders to be allowed to enter the United States); Act of Sept. 22, 1959, Pub. L. No. 86-363, 73 Stat. 644 (facilitating the entry of fiancées and relatives of alien residents and U.S. citizens); Act of Oct. 3, 1965, Pub. L. No. 89-236, 79 Stat. 911 (abolishing the earlier quota system centered on national origins, focusing instead on reuniting families and attracting skilled labor, but still placing a cap on immigration from certain countries and on total immigration, as well as on each category of immigrants); Refugee Act of 1980, Pub. L. No. 96-212, 94 Stat. 102 (providing a procedure for humanitarian aid to be given to refugees from areas of particular interest to the United States); Immigration Act of 1990, Pub. L. No. 101-649, 104 Stat. 4978 (reforming the Immigration and Nationality Act of 1965 by revising the preference categories and dividing immigrants into three categories: family-sponsored, employment-based, and diversity). A few measures focused on the structure of the immigration agencies and the border patrol. *See, e.g.*, Act of May 28, 1924, Pub. L. No. 68-153, 43 Stat. 240 (establishing the U.S. Border Patrol); Act of June 4, 1940, ch. 231, 54 Stat. 230 (transferring the Immigration and Naturalization Service from the Department of Labor to the Department of Justice).

establishing identity, encouraging individuals from certain countries (or with experience in skilled industries or strong connections to the United States) to immigrate, while prohibiting other classes of aliens considered undesirable or a threat to the country. A few measures expanded the classes of deportable offenses, such as those directed at aliens convicted of crimes related to weapons, bombs, or illegal drugs, those who had perpetrated fraud to gain entry, and illegal immigrants.[157]

By the beginning of the twenty-first century, the role of immigration inspectors had expanded to include: inspecting and admitting individuals arriving at ports of entry; administering benefits (such as naturalization); granting asylum; patrolling the borders; and apprehending and removing aliens who enter illegally, violate requirements of their admission, or present a threat.[158] The emphasis throughout this time, and continuing to the present day, was on ascertaining the identity and citizenship of U.S. citizens and aliens seeking entry to the United States.

As the Supreme Court has recognized, citizens and individuals with a substantial connection to the United States benefit from the protections of the Fourth Amendment in their interactions with immigration officials.[159] Non-U.S. persons lacking these characteristics, however, have no such rights. Immigration officials thus have broader authorities as to aliens: they can be interrogated, arrested, and subjected to more intrusive searches, including searches, "without warrant, of the person and of [their] personal effects," where the immigration officer has "reasonable cause to suspect that grounds exist for denial of admission to the United States."[160] Congress, to date, has not made any special exceptions for the personal effects that may be searched. As a result, guidance on electronic devices has been left to the agencies themselves.

Despite the broader leeway provided to search of aliens, as with customs measures, the law still recognizes the greater privacy protections afforded to the home, as well as the application of the Fourth Amendment within U.S. borders.

---

157. *See, e.g.*, Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359 (providing amnesty as well as deportation authorities) (codified as amended in scattered sections of 8 U.S.C.); Alien Registration Act, Pub. L. No 76-670, 54 Stat. 670 (1940) (expanding deportable classes to include smuggling, aiding in illegal entry, and membership in proscribed organizations and subversion) (codified at 18 U.S.C. § 2385 (2018)); Act of May 14, 1937, Pub. L. No. 75-79, 50 Stat. 164 (making deportable aliens who secured a visa through fraud); Act of Feb. 18, 1931, Pub. L. No. 71-683, 46 Stat. 1171 (establishing deportability for convictions related to import, export, manufacture, or sale of heroin, opium, or coca leaves); Act of Mar. 4, 1929, Pub. L. No. 70-1018, 45 Stat. 1551 (establishing deportability of aliens for convictions related to weapons or bombs).

158. USCIS Report, *supra* note 133, at 10.

159. United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

160. 8 U.S.C.A. § 1357(a), (c) (West 2018).

Thus, even though immigration authorities have the power to search for aliens domestically, the law requires either consent or a properly-executed warrant to enter onto farm land or any agricultural operation to interrogate individuals as to their right to be in the United States.[161]

IV. APPLICABLE FOURTH AMENDMENT DOCTRINE

As CBP and ICE have made increasing use of their border search authorities, calls to exempt electronic devices from the exception to the warrant requirement have increased.[162] The argument is that these devices contain a tremendous amount of private information not accessible in a routine border search. Prior to the Supreme Court's decisions in *Riley v. California*, *United States v. Jones*, and *Carpenter v. United States*, courts generally rejected the argument based on the grounds that the search was routine and did not require reasonable suspicion (pursuant to the border search exception), or that the actual search in question had been conducted with reasonable suspicion.[163] However, a few courts did determine that forensic examination required a higher standard.[164] Since *Riley* and *Carpenter*, more courts have questioned—and rejected—unfettered access to citizens' electronic devices.[165] These courts are correct. The Fourth Amendment places a limit on the search of electronic devices, at least as to U.S. persons and individuals who have a substantial connection to the United States.

---

161. 8 U.S.C. § 1357(e) (2018). But note that lower courts have held that the "reasonable distance" provision, which allows the Attorney General to determine the distance from the border at which probable cause and a warrant are required, is constitutional even though it does not insert a neutral magistrate into the review process. United States v. King, 485 F.2d 353 (10th Cir. 1973), *rev'd on other grounds*, Bowen v. United States, 422 U.S. 916 (1975).

162. *See, e.g.*, Sophia Cope & Adam Schwartz, *EFF's Fight to End Warrantless Searches at the Border: A Roundup of Our Advocacy*, ELECTRONIC FRONTIER FOUND. (Jan. 26, 2018), https://www.eff.org/deeplinks/2018/01/round-effs-advocacy-against-border-device-searches [https://perma.cc/A2V7-WWCZ]; Charlie Savage and 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 [https://perma.cc/5HS3-8CL2]; *Warrantless Border Searches Expand as Courts Grapple with Growing Legal Implications*, A.B.A. (Aug. 3, 2018), https://www.americanbar.org/news/abanews/aba-news-archives/2018/08/warrantless_borders [https://perma.cc/RNG5-C6LL].

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

164. United States v. Cotterman, 709 F.3d 962, 962-68 (9th Cir. 2013) (en banc); United States v. Saboonchi, 990 F. Supp. 2d 536, 564-71 (D. Md. 2014).

165. *See, e.g.*, United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); United States v. Molina-Isidoro 884 F.3d 287 (5th Cir. 2018); United States v. Kim, 103 F. Supp. 3d 32, 54 (D.D.C. 2015); *see also* United States v. Vergara, 884 F.3d 1309 (11th Cir. 2018) (Pryor, J., dissenting).

A. Cases Before Riley *and* Carpenter

Although the Supreme Court in *Flores-Montano* left open the possibility, under certain circumstances, that reasonable suspicion could be required for certain property searches at the border,[166] several courts, prior to *Riley* and *Carpenter*, considered the search of electronic devices to fall within the ordinary border search exception. Others determined that in the particular case before them, reasonable suspicion had been met. Still others extended special protections to forensic searches.

1. Cases Holding Electronic Border Searches Are Not Subject to Reasonable Suspicion

Several of the cases permitting electronic border searches without reasonable suspicion derive from incidents involving child pornography. In *United States v. Arnold*, for instance, a traveler named Michael Arnold arrived at Los Angeles International Airport after a nearly twenty-hour flight from the Philippines.[167] When Arnold went to clear customs, CBP pulled him aside for secondary questioning, inspected his luggage, and found a laptop, a separate hard drive, a USB stick, and six disks. Agents directed him to turn on his computer. On the desktop, agents found folders labeled "Kodak Pictures" and "Kodak Memories." When agents opened the folders, they found photos of naked women. CBP called in ICE, who, believing the pictures to include children, detained and questioned the traveler. They seized his computer and the storage devices and, two weeks later, obtained a warrant. The Department of Justice charged Arnold with transporting child pornography.

Despite the amount of information that could be held on the computer, the court did not see that the search raised any Fourth Amendment concerns. Neither of the narrow grounds laid out by the Supreme Court in *Flores-Montano* that would require reasonable suspicion ("exceptional damage to property" or "particularly offensive manner") applied.[168] The court was "satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."[169] When a similar case arose in regard to fraudulent alien cards, which were found on a traveler's hard

166. United States v. Flores-Montano, 541 U.S. 149, 155-56 (2004).

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

168. *Id.* at 1008-09.

169. *Id.* at 1008.

drive while crossing the border, the Ninth Circuit considered the requirement of reasonable suspicion to be foreclosed by *Arnold*.[170]

The Fourth Circuit reached a similar conclusion in *United States v. Ickes*.[171] In that case, the defendant, driving a van that appeared to be packed with everything he owned, crossed the U.S.-Canada border. A search of the van uncovered a video camera with a tape of a tennis match in which the camera was focused on a young ball boy. Border agents found marijuana seeds and pipes and several photo albums of child pornography. They also found a computer and seventy-five diskettes with additional child pornography on them. The court ruled the search permissible on the grounds that "[b]oth Congress and the Supreme Court have made clear that extensive searches at the border are permitted, even if the same search elsewhere would not be."[172] At least one other published lower court opinion reached a similar conclusion.[173]

2. *Cases Finding that the Search Was Supported by Reasonable Suspicion*

Unlike *Arnold* and the cases where the judiciary has dispensed with the reasonable suspicion requirement, in other instances, courts ruled that reasonable suspicion of criminal activity was present at the time of the electronic search. The first set of cases stemmed from ongoing criminal investigations related to the traveler that agents became aware of during the border encounter; the second derived from agents observing suspicious activity or uncovering illegal substances during the individual's transit.

In *United States v. Hassanshahi*, a traveler's laptop was seized during an international border stop at a U.S. airport.[174] An inquiry into the traveler's identity revealed he was the subject of an ongoing federal investigation into a conspiracy to build a computer production facility in Iran in violation of U.S. trade embargoes. The court in that case considered agents to have established reasonable suspicion sufficient to support a forensic examination of the laptop.[175] Similarly, in *United States v. Saboonchi*, a traveler's name came up in

170. United States v. Singh, 295 F. App'x 190, 191 (9th Cir. 2008).

171. 393 F.3d 501 (4th Cir. 2005).

172. *Id.* at 502-03.

173. *See, e.g.*, United States v. McAuley, 563 F. Supp. 2d 672, 673-75 (W.D. Tex. 2008) *aff'd*, 420 Fed. App'x 400 (5th Cir. 2011). In *United States v. Hampe*, the court held that the search of a laptop was a routine search and that reasonable suspicion was not required, but it then concluded that the particular facts of the case gave rise to reasonable suspicion that child pornography was involved. Crim. No. 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007), *adopted by*, 2007 WL 1806671 (D. Me. June 19, 2007).

174. United States v. Hassanshahi, 75 F. Supp. 3d 101 (D.D.C. 2014).

175. *Id.* at 107.

connection with two different export violation investigations.[176] The government had information that the defendant had purchased two cyclone separators that had then been shipped overseas to an entity linked to a company in Iran. The court determined that the forensic search of the defendant's smart phone and flash drive had been supported by reasonable suspicion.[177] Meanwhile, in *United States v. Cotterman*, the Ninth Circuit determined that border agents had reasonable suspicion for their initial search because the defendant had a prior conviction for child molestation, frequently traveled to a country associated with sex tourism, and carried password-protected files.[178] A handful of lower courts found the presence of illegal substances during the search to be sufficient for the examination of electronic devices.[179]

3. Cases Extending Special Protections to Forensic Investigations

A third category of cases prior to *Riley* and *Carpenter* extended Fourth Amendment protections to more intrusive forensic investigations. The most prominent case came out of the Ninth Circuit. In *United States v. Cotterman*, agents entered a traveler's name into the Treasury Enforcement Communication System (TECS), which revealed a 15-year old child sexual molestation charge. Agents referred the defendant and his wife for secondary questioning, ordering them to leave their car and belongings behind. A search of the vehicle yielded two laptop computers with password-protected files. The defendant offered to assist agents in accessing the information, but the agents declined because of concern that the defendant would use the opportunity to sabotage the files. Agents seized the computers and transported them to Tucson, 150 miles away,

176. United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014).

177. *Id.* at 571.

178. United States v. Cotterman, 709 F.3d 952, 970 (9th Cir. 2013) (en banc).

179. *See, e.g.*, United States v. Mendez, 240 F. Supp. 3d 1005 (D. Ariz. 2017) (finding reasonable suspicion for a mobile phone search at the border after the discovery of drugs in a car); United States v. Molina-Isidoro, 267 F. Supp. 3d 900 (W.D. Tex. 2016) (permitting mobile phone search with reasonable suspicion at Mexican border after agents found methamphetamine in the traveler's suitcase); United States v. Cano, 222 F. Supp. 3d 876 (S.D. Cal. 2016) (finding reasonable suspicion to download mobile phone data on grounds that it had been used as an instrumentality of the crime where agents had found sixteen kilograms of cocaine in the spare tire of the defendant's truck); United States v. Ramos, 190 F. Supp. 3d 992 (S.D. Cal. 2016) (determining that DHS's manual search of a phone and examination of incoming calls, text messages, and the call log was reasonable after agents had found methamphetamine in the car and questioned defendant, who said he had been in cell phone communication with a person to whom he was reporting); United States v. Caballero, 178 F. Supp. 3d 1008 (S.D. Cal. 2016) (finding that reasonable, particularized suspicion was present where CBP found illegal drugs in defendant's car and searched the defendant's mobile phone, which had photos of large sums of money).

for forensic evaluation. Over the course of three days, agents found seventy-five images of child pornography.[180]

The court determined that border searches must be limited in time and distance: agents needed to have reasonable suspicion that the subject was involved in criminal activity. Further, mere suspicion was not enough to justify a search.[181] The court recognized the unique nature of the type of information contained in electronic devices:

> The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. This is no longer the case. Electronic devices are capable of storing warehouses full of information . . . . Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails . . . . Electronic devices often retain sensitive and confidential information far beyond the perceived point of erasure, notably in the form of browsing histories and records of deleted files. This quality makes it impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel.[182]

A second case, this time in the District of Maryland, held that the forensic border search of any computer or electronic device should be considered nonroutine and therefore require reasonable suspicion.[183] The court's justification was that, while the government has legitimate concerns about child pornography, those concerns do not justify an unregulated assault on citizens' private information—which is what is involved in forensic examination of a hard drive.[184]

In *United States v. Saboonchi*, the court took a different approach than that followed in *Cotterman*, where the court had determined that the forensic search of a computer that had been imaged was as invasive of the defendant's privacy as a strip search.[185] The *Saboonchi* court took issue with the Ninth Circuit's failure to provide guidelines for what constituted a "forensic" search. Distinguishing between routine and nonroutine border searches, the court tried

180. *Cotterman*, 709 F.3d at 957-59.

181. *Id.* at 962-68 (requiring reasonable suspicion for forensic examination of the laptop).

182. *Id.* at 964-65.

183. United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014).

184. *Cotterman*, 709 F.3d at 966.

185. *Id.*

to construct a test for determining when a conventional computer search becomes a forensic investigation:

> A conventional search at the border of a computer or device may include a Customs officer booting it up and operating it to review its contents, and seemingly, also would allow (but is not necessarily limited to) reviewing a computer's directory tree or using its search functions to seek out and view the contents of specific files or file types . . . . And, just as a luggage lock does not render the contents of a suitcase immune from search, a password protected file is not unsearchable on that basis alone.[186]

In contrast, the *Saboonchi* court said, a forensic search involves the creation of a bitstream copy that is then "searched by an expert using highly specialized analytical software—often over the course of several days, weeks or months—to locate specific files, [] recover hidden, deleted, or encrypted data, and analyze the structure of files" and the drive.[187] The court provided three explanations for why forensic searches should be considered sui generis: first, such a search creates a copy and uses specialized software to analyze the computer's contents, creating the potential for an unbounded search; second, it provides access to deleted material; and third, it provides insight into an individual's actions away from the border that would not otherwise be discoverable.[188]

In a similar vein, the First Circuit, in evaluating other kinds of searches, has offered the following nonexhaustive list of factors that may be relevant when determining whether a search can be characterized as routine:

> (i) whether the search results in the exposure of intimate body parts or requires the suspect to disrobe; (ii) whether physical contact between Customs officials and the suspect occurs during the search; (iii) whether force is used to effect the search; (iv) whether the type of search exposes the suspect to pain or danger; (v) the overall manner in which the search is conducted; and (vi) whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search.[189]

These factors appear to be directed towards ascertaining the degree of intrusiveness of the search and its affect on the traveler—elements central to Fourth Amendment concerns.

---

186. *Saboonchi*, 990 F. Supp. 2d at 560-61.

187. *Id.* at 561.

188. *Id.* at 564; *see also* Gretchen C.F. Shappert, *The Border Search Doctrine: Warrantless Searches of Electronic Devices After* Riley v. California, U.S. ATT'Y'S BULL., Nov. 2014, at 10.

189. United States v. Braks, 842 F.2d 509, 512 (1st Cir. 1988) (footnotes omitted).

B. Riley v. California*: Stronger Constitutional Protections for Mobile Devices*

The above cases predated *Riley v. California*, in which the Supreme Court recognized the unique incursions into privacy occasioned by the search of a mobile device.[190] In holding that search of a cell phone incident to arrest required a warrant supported by probable cause, the Court underscored the distinction between electronic devices and other, physical items. The sheer capacity of mobile devices had important implications for privacy.[191]

In *Riley*, the court noted that more than ninety percent of American adults own and carry cell phones, keeping "on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[192] The type of information gleaned differs in important respects from what can be uncovered from physical search. Cell phones contain medical records, location information, relationship details, political beliefs, religious convictions—in fact, more than could be ascertained even from the search of an individual's home.[193] Beyond this, mobile phones provide a gateway to vast amounts of data stored remotely in the cloud. The Court in *Riley* was unsatisfied with the government's proposal to "disconnect a phone from the network before searching the device,"[194] which CBP has adopted for electronic border searches. For the Court, even disconnected from the cloud, mobile phones contained vast amounts of private data.

One of the first border search cases to apply *Riley* was *United States v. Kim*, in which the court determined that the question of electronic searches was settled neither by the border exception nor by application of what was meant by

---

190. Riley v. California, 134 S. Ct. 2473 (2014). There were two cases on appeal in *Riley*. *See* United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *reh'g en banc denied*, No. 11-1792, 2013 WL 4080123 (1st Cir. July 29, 2013). In *Wurie*, the First Circuit held that the search incident to arrest exception did not authorize the warrantless search of a mobile telephone. *Id.* at 13. Quoting the Seventh Circuit, the court observed that "[a]t the touch of a button a cell phone search becomes a house search, and that is not a search of a 'container' in any normal sense of that word, though a house contains data." *Id.* at 8-9 (quoting United States v. Flores-Lopez, 670 F.3d 803, 806 (7th Cir. 2012)). The First Circuit, however, rejected the Seventh Circuit's final determination, concluding that cell phone search incident to arrest was not supported by the justification in *Chimel v. California*, 395 U.S. 752 (1969). There, the Court permitted police arresting a person in their home to search the area within immediate reach of the person. The First Circuit also determined that the scope of the information obtained exceeded the purpose of the warrant exception. *Id.* at 8-12.

191. *Riley*, 134 S. Ct. at 2489.

192. *Id.* at 2490.

193. *Id.* at 2490-91.

194. *Id.* at 2491.

"forensic."[195] Instead, the court in *Kim* considered the extent to which the search "intrudes upon an individual's privacy on the one hand, and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[196] The court noted:

> [W]hile the courts in *Ickes*, *Cotterman*, and *Saboonchi* had little in the way of Supreme Court precedent to guide their way, the Supreme Court has since issued its opinion in *Riley v. California*. And in *Riley*, the Court made it clear that the breadth and volume of data stored on computers and other smart devices make today's technology different in ways that have serious implications for the Fourth Amendment analysis.[197]

Under a totality of circumstances test, the court found that the imaging and search of a laptop, for an unlimited period and without any limits on the scope of the analysis, invaded the traveler's privacy to such an extent that it was unreasonable under the Fourth Amendment.[198] The court noted that "given the vast storage capacity of even the most basic laptops, and the capacity of computers to retain metadata and even deleted material, one cannot treat an electronic storage device like a handbag simply because you can put things in it and then carry it onto a plane."[199]

The *Kim* case is notable not just for its application of *Riley*, but because it involved a decision by investigators to wait until a suspect left the United States before using the border exception to search his laptop and thereby obtain detailed information about his activities.[200] The court ultimately rejected the agents' approach of using the border search exception to obtain information to which they otherwise would not be entitled.[201]

---

195. United States v. Kim, 103 F. Supp. 3d 32, 54 (D.D.C. 2015).

196. *Id.* at 55 (quoting *Riley*, 134 S. Ct. at 2484).

197. *Id.* at 54.

198. *Id.* at 59.

199. *Id.* at 50.

200. *Id.* at 38-39. *Riley*'s treatment of electronic devices has influenced judicial analysis of not just the border exception, but other doctrinal Fourth Amendment exceptions. *See, e.g.*, United States v. Lara, 815 F.3d 605, 610-12 (9th Cir. 2016) (applying *Riley* to probation officers' searches); United States v. Camou, 773 F.3d 932, 942-43 (9th Cir. 2014) (applying *Riley* to the vehicle search exception); *cf.* United States v. Henry, 827 F.3d 16, 28 (1st Cir. 2016) (rejecting *Riley* in the plain view context because law enforcement had obtained a warrant prior to search of the phone).

201. *Id.* at 45 (citing United States v. Hassanshahi, 75 F. Supp. 3d 101, 120-21 (D.D.C. 2014)).

Despite *Kim*, the government has argued that the courts have "repeatedly rejected" applying *Riley* to the border search exception.[202] That statement is misleading: while a number of Ninth Circuit lower court cases have not applied *Riley*, they are bound by *Cotterman* unless the court finds the two cases to be "clearly irreconcilable."[203] Similarly, lower courts in the Fourth Circuit are subject to *Ickes*.[204]

Other courts post-*Riley* have considered forensic examination of mobile phones to be nonroutine and have allowed searches only upon a showing of individualized suspicion or probable cause. In *United States v. Kolsuz*, the Fourth Circuit held that the forensic border search of a mobile device required individualized suspicion.[205] In that case, Mr. Kolsuz was detained when CBP uncovered firearms parts in his luggage.[206] Agents seized his phone and subjected it to a month-long forensic examination, generating a nearly 900-page report on the contents of the device. The district court determined that, under *Riley*, the forensic investigation was nonroutine but justified by reasonable suspicion.[207] The Fourth Circuit agreed that nonroutine searches require some level of individualized suspicion. It did not, however, reach the question of whether reasonable suspicion was sufficient, or if probable cause was required.[208] Because probable cause had been present, the good faith exception applied and the court was not required to suppress the information.

In *United States v. Molina-Isidoro*, the Fifth Circuit declined to announce a rule regarding the application of the border search exception to the modern technologies for which the Supreme Court, in *Riley*, had recognized increased

---

202. *See, e.g.*, Memorandum in Support of Defendants' Motion to Dismiss at 25, Alasaad v. Nielsen, No. 17-CV-11730-DJC (D. Mass. Dec. 15, 2017).

203. United States v. Caballero, 178 F. Supp. 3d 1008, 1018 (S.D. Cal. 2016) ("Although *Riley* could be applied to a cell phone search at the border, this Court is bound by *Cotterman*.") (citing United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013)); *see also* United States v. Mendez, 240 F. Supp. 3d 1005, 1008 (D. Ariz. 2017); United States v. Ramos, 190 F. Supp. 3d 992, 1002-03 (S.D. Cal. 2016); United States v. Cano, 222 F. Supp. 3d 876, 878 (S.D. Cal. 2016); United States v. Hernandez, No. 15-CR-2613-GPC, 2016 WL 471943, at *3 n.2 (S.D. Cal. Feb. 8, 2016); United States v. Lopez, No. 13-CR-2092-WQH, 2016 WL 7370030, at *5 (S.D. Cal. Dec. 20, 2016). *But see* United States v. Escarcega, 685 Fed. App'x 354 (5th Cir. 2017); United States v. Feiten, No. 15-20631, 2016 WL 894452, at *6 (E.D. Mich. Mar. 9, 2016); United States v. Blue, No. 1-14-CR-244-SCJ, 2015 WL 1519159, at *2 (N.D. Ga. April 1, 2015).

204. United States v. Ickes, 393 F.3d 501, 505-06 (4th Cir. 2005).

205. 890 F.3d 133 (4th Cir. 2018).

206. *Id.* at 136.

207. *Id.*; *see also* United States v. Kolsuz, 185 F. Supp. 3d 843, 856 (E.D. Va. 2016) (using *Riley* to evaluate the privacy interest at stake).

208. 890 F.3d at 136.

privacy interests.[209] Its rationale is of note: having found several kilos of methamphetamine in the traveler's suitcase, CBP looked at some applications on her phone. According to the court, "the nonforensic search of Molina-Isidoro's cell phone at the border was supported by probable cause. That means, at a minimum, the agents had a good-faith basis for believing the search did not run afoul of the Fourth Amendment."[210]

In *United States v. Vergara*, a divided Eleventh Circuit panel considered the warrantless forensic search of three phones at the border.[211] The majority stated: "Border searches 'never' require probable cause or a warrant. And we require reasonable suspicion at the border only 'for highly intrusive searches of a person's body such as a strip search or an x-ray examination.'"[212] Judge Jill Pryor, dissenting, agreed "that the government's interest in protecting the nation is at its peak at the border," but she faulted the majority for ignoring the implications of *Riley*.[213] In her view, "a forensic search of a cell phone at the border requires a warrant supported by probable cause."[214]

C. *The Effect of* Carpenter v. United States

As with *Riley*, the Court's decision in *Carpenter v. United States* has implications for how to think about electronic border searches.[215] In that case, a man arrested for a series of robberies provided the mobile telephone numbers of his alleged accomplices to the FBI.[216] Prosecutors applied for a court order under the Stored Communications Act to direct service providers to supply them with "[a]ll subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target

209. 884 F.3d 287 (5th Cir. 2018).

210. *Id.* at 289.

211. United States v. Vergara, 884 F.3d 1309 (11th Cir. 2018), *cert. denied*, No. 16-15059 (Oct. 1, 2018).

212. *Id.* at 1312 (quoting United States v. Ramsey, 431 U.S. 606, 619 (1977)); *see also* United States v. Touset, 890 F.3d 1227 (11th Cir. 2018). In *Touset*, Judge William Pryor reached the same conclusion as in *Vergara*, applying the case to another border search of a mobile device, and stating that an agent's search of electronic devices at the border does not need to be based on suspicion and, in any event, reasonable suspicion was present in this case.

213. 884 F.3d at 1313 (Pryor, J., dissenting).

214. *Id*.

215. Carpenter v. United States, 138 S. Ct. 2206 (2018).

216. *Id.* at 2212.

telephones" as well as "cell site information for the target telephones . . . for incoming and outgoing calls" for the suspects.[217]

Concerned by the volume and intrusiveness of location information, the Court created an exception to third-party doctrine.[218] Its reasoning built on the so-called "shadow majority" in *United States v. Jones*, in which five justices adopted the view that individuals have a reasonable expectation of privacy in the whole of their physical movements.[219] For the Court, the purpose of the Fourth Amendment was to secure the privacies of life from arbitrary power and to place obstacles in the way of excessive government surveillance.[220] Over the years, technology had repeatedly disrupted that balance. Justice Roberts, citing Justice Brandeis's dissent in *Olmstead v. United States*, explained that as "more far-reaching means of invading privacy . . . become available to the Government," it was up to the Court "to ensure that the 'progress of science' does not erode Fourth Amendment protections."[221] Just as *Kyllo v. United States* responded to sense-enhancing technology (in that case, thermal imaging),[222] *Riley* had recognized the "vast store of sensitive information" available on a mobile device.[223] In jettisoning the application of the third-party doctrine to geolocational data, the Court focused on two areas: the nature of the documents being sought and limitations on any legitimate expectations of privacy. Both factors should shape border search doctrine going forward.[224]

1. Nature of Documents Being Sought

In examining the nature of the documents sought, Chief Justice Roberts first looked at the number of people implicated, observing that there are approximately 400 million electronic devices in the United States, making virtually everyone in America subject to the provisions.[225] The Court

217. *Id.*; *see also* 18 U.S.C. § 2703(d) (2018); United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016).

218. *Carpenter*, 138 S. Ct. at 2217, 2223; *see* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976); *see also* Donohue, *supra* note 113; Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 NYU ANN. SURV. AM. L. 553 (2017).

219. United States v. Jones, 565 U.S. 400 (2012).

220. *Carpenter*, 138 S. Ct. at 2214.

221. *Id.* at 2223 (citing Olmstead v. United States, 277 U.S. 438, 473-74 (1928)).

222. *Id.* at 2214 (citing Kyllo v. United States, 533 U.S. 27, 34, 35 (2001)).

223. *Id.* (citing Riley v. California, 134 S. Ct. 2473, 2489, 2484 (2014)).

224. In addition to the factors considered in this Essay, significant property interest rights are present in the context of border searches. For a detailed discussion of how to read the Fourth Amendment in this context, see Donohue, *supra* note 113.

225. *Carpenter*, 138 S. Ct. at 2218.

acknowledged that the type of information at stake conveyed the intimate details of one's life. It was "detailed, encyclopedic, and effortlessly compiled,"[226] — not unlike the massive amount of information contained on a mobile phone, iPad, or computer. It provided near perfect recall, making the data different than information that could be conveyed by another individual — even a party to the underlying action in question.[227] The fact that the information was broad and increasingly more nuanced mattered, as did the fact that the resource constraints on obtaining such information were falling away.[228] The Court noted its concern that the information was retroactive, giving "police access to a category of information otherwise unknowable."[229] Based on these observations, the Court determined that the data at issue was particularly sensitive and therefore deserved protections not afforded by third-party doctrine.

Each of the factors highlighted by the Court applies to the search of mobile devices at the border. Most people entering or leaving the country carry their electronic devices with them to satisfy a host of logistical and recreational needs. Travelers also need their devices once they reach their destination. This information provides deep insight into the most intimate aspects of travelers' lives.

It is possible, of course, for users to delete all of the information from their devices, to place it on a hard drive or on the cloud, and to later restore it; or, alternatively, to use a different telephone or laptop devoid of any private information. But in addition to contradicting the basic Fourth Amendment position articulated by the Court in *Carpenter*, it would be an unreasonable expectation and one with numerous harmful consequences. For instance, it may be expensive to purchase a hard drive or cloud access, or to rent (or buy) an alternative device. At the very least, it would take time and may well exceed the average traveler's technological knowledge. For individuals who use their travel time to work, to answer email, or to prepare for meetings, deleting this information would be highly disruptive and result in a detrimental impact on productivity. For those using the devices for personal or social reasons, they would be unable to do so while en route. Such an approach would essentially create a technological black hole at the border, while opening up the possibility that all travelers' data could be intercepted when they restore information overseas. Alternatively, while overseas, citizens might lose access to possibly vitally-important data, unless they could access the cloud. One possible counterargument is that travelers could simply place their devices in airplane

226. *Id.* at 2216; *see also id.* at 2220.

227. *Id.* at 2219.

228. *Id.* at 2217, 2218-19.

229. *Id.* at 2218.

mode. But this does nothing to eliminate access to everything held on the device itself, which the Court in *Riley* was at pains to note included the full range of the privacies of life.

The Court in *Carpenter*, moreover, acknowledged the privacy interests at stake in geolocational data in particular. Most mobile devices contain GPS chips, which allow them to communicate with satellites to pinpoint a user's location. Location data can then be logged by the device and various applications. Google Maps, for example, logs your information as you move and stores where you have been. That history is accessible to anyone who accesses the device. Social media platforms like Foursquare, Twitter, or Facebook include location information when you post.[230] Location data, unless expressly turned off, is further embedded in photographs and videos as geotags—i.e., the precise longitude and latitude of where the photo was taken—and time stamps. Under *Carpenter*, search of this information is a search for Fourth Amendment purposes, and it requires a warrant, supported by probable cause, to access it for seven days or more.[231]

The same characteristics of geolocational data, additionally, apply to the myriad types of information held on an electronic device. They incorporate calendars, address books, private correspondence, financial records, memos, and documents of every sort, as well as pictures, books travelers have read or are reading, and detailed information on intimate relationships. Like cell site location information (CSLI), such information is "detailed, encyclopedic, and effortlessly compiled."[232] For the Court in *Carpenter*, the level of detail and precision and retroactive nature of the data all mattered. By using the map function or the GPS chip, the government can not only "travel back in time to retrace a person's whereabouts,"[233] but can also access all of the user's correspondence—for decades, possibly—even when the user has tried to delete this information from their laptop. In searching electronic devices, the government can access data not just for information held on the actual machine, but for data stored in the cloud. The upshot is that the government, without any probable cause, can subject an individual's entire life to scrutiny, bypassing the Fourth Amendment altogether. As for the diminishing resource constraints, this is no less true of border searches: where before the government would have had to obtain a warrant, send officers, and knock and announce at a home before

230. So many people are unaware of this feature that the website PleaseRobMe.com has been created to inform people and to teach them how to turn it off. *See Raising Awareness About Over-Sharing*, http://pleaserobme.com [https://perma.cc/936Q-GZKE].

231. *Carpenter*, 138 S. Ct. at 2217.

232. *Id.* at 2216.

233. *Id.* at 2218.

entering to search, now, at the push of a button, all of the information that could have otherwise been obtained from the home—plus a great deal more—can be collected from electronic devices at the border.

2. Legitimate Expectations of Privacy

The second aspect of the Court's inquiry regarding the expectation of privacy with respect to geolocational data is no less relevant to border search of electronic devices writ large. The Court noted that location data was not in any sense voluntarily shared. Mobile phones have become such a pervasive part of life that they are not optional.[234] The Court further acknowledged that individuals do not have to do anything to have their location recorded by the service provider, nor is it an option not to create a record.[235] Therefore, in no meaningful sense is there an assumption of risk.[236]

In obtaining information during a border search *directly from the phone itself*, and not from the service provider, the third-party doctrine drops away altogether. As for the argument that a traveler assumes the risk that border agents will search their electronic devices, only one of two options might apply.

First, the argument could be made that, by using an electronic device, an individual summarily consents to, or assumes the risk that, the government will search it. But this is plainly not true.[237] Individuals do not knowingly and voluntarily share their lives with the government simply by using digital devices. Mobile phones, tablets, and computers are private, often encrypted, and protected by multiple passwords for different applications. The devices are stored inside the home, often replacing many of the records that would otherwise be documented on paper and placed in filing cabinets and drawers. And consumers demand that providers exercise network security. As ours has become a digital world, these documents have evolved, but their essential quality remains. Simply by living in the modern world, individuals do not assume a new risk that the government will gain access to their most sensitive information. Such logic flies in the face of the Court's holding in *Riley*.

The second possibility would be that by moving or traveling with an electronic device *across the border*, individuals assume the risk that their entire

234. *Id.* at 2200 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").

235. *Id.*

236. *Id.* ("[I]n no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements.") (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

237. This argument also erroneously imports an analogy from informant doctrine. *See* Donohue, *supra* note 113.

lives will be examined by the government. But it is contradictory to say that mobile electronic devices have become an integral part of life, such that it is necessary to have them to live in the modern world, and then to say that such devices are optional when one travels abroad. They are not. This argument also does not comport with the Fourth Amendment's prohibition on general warrants, as was recognized in the Supreme Court's holding in *Verdugo-Urquidez*.[238] U.S. citizens do not forfeit their Fourth Amendment rights when they travel overseas. The government's argument would create a Constitution-free zone at every port of entry, where citizens have Fourth Amendment rights inside and outside the United States, but not as they cross the border. That is not how the Constitution works. It applies to the people of the United States at all times. Just as the fact that the geolocational records in *Carpenter* were obtained from a third party was not enough to overcome Fourth Amendment interests,[239] so too is the fact that an electronic search occurs at the border insufficient to overcome citizens' constitutional rights.

D. Digital Communications and Electronic Mail

As was detailed earlier in this Essay, special protections extend to the transfer of physical mail across the border. These further illustrate the extent to which CBP and ICE practices in regard to digital communications run afoul of constitutional limits—a limit explicitly recognized by the Court in *Carpenter* as a modern analogue.[240]

As aforementioned, officials inspecting mail that weighs less than sixteen ounces must first obtain a warrant to ensure that Fourth Amendment standards are met. This rule provides a sharp contrast to CBP's current practice regarding email. To be sure, warrants are not required for paper correspondence unless the mail is sealed. But the equivalent in the digital realm is use of a password or encryption. At present, though, CBP policy permits agents to read travelers' emails with no suspicion of any wrongdoing whatsoever, and, under the current regulations, CBP and ICE can insist that travelers provide the passwords to their electronic devices. Barring cooperation, they can simply keep the machines and use sophisticated techniques to bypass the protections otherwise instituted to keep prying eyes from seeing personal information.

The distinction between the protections afforded digital and paper correspondence does not track the relevant privacy interests, which apply equally

238. United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

239. *Carpenter*, 138 S. Ct. at 2200.

240. *Id.* at 2222 (citing and quoting *id*. at 2230 (Kennedy, J., dissenting)) (citing United States v. Warshak, 631 F.3d 266, 283-88 (6th Cir. 2010)).

to many forms of digital communications: from emails and text messages, to communications embedded in applications such as Instagram or WhatsApp Messenger. Regardless of the medium, they memorialize the substance of communications between individuals that would be protected under the Fourth Amendment if it were written on paper. While the sealing of the envelope plays a key role in the doctrine for paper correspondence, there is no relevant difference in a traveler's decision to password-protect electronic devices as well as access to email, text messages, or applications.

While the Fourth Amendment requires only reasonable suspicion to access to mail that weighs more than sixteen ounces or for trunks or envelopes on board vessels transiting the border,[241] that standard is still higher than that currently required for border searches of electronic devices. For the latter, *no* suspicion whatsoever is required. In addition, postal provisions that allow the government to search mail weighing over sixteen ounces or trunks or envelopes on board vessels, only allow officials to look for money, weapons of mass destruction, or contraband falling into one of the six categories. Even then, the government may only search for contraband based on reasonable suspicion of uncustomed goods. No provision permits monitoring for criminal or political activity writ large. Yet such searches are entirely consistent with the current regime governing electronic search at the border, regardless of the volume or extent of the files being inspected.

V. DIGITAL CONTRABAND, CUSTOMS, AND IMMIGRATION

Customs and immigration both deal with the movement of physical objects. As this Essay has explained, the purpose behind these regimes is not to identify general criminal activity.[242] It is to prevent contraband and uncustomed goods from crossing the border, and to ascertain the identity and citizenship of individuals seeking entry to determine whether to admit foreign nationals.[243] Before concluding, it is important to narrow the discussion to recognize two potential challenges grounded in the legitimate interests of CBP and ICE.

241. United States v. Ramsey, 431 U.S. 606, 612 (1977).

242. United States v. Seljan, 547 F.3d 993, 1001 (9th Cir. 2008) (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985)).

243. CBP recognizes these objectives in the guidance it provides to travelers whose devices are detained for examination. *See Inspection of Electronic Devices*, *supra* note 10.

A. Illegal Goods

How *should* we think about illicit materials that happen to be digitized? A strong argument could be mounted that digital contraband, after all, is still contraband and thus well within CBP's domain. This is a sort of reverse of the functional rule of equivalence that I have elsewhere argued should govern the Court's Fourth Amendment jurisprudence.[244] Applied in this context, the argument runs: digital contraband still functions as material that Congress has prohibited, often because of the risk of harm. Just because something is carried on an iPad, instead of inside a knapsack, its purpose does not necessarily alter. So why should it enjoy a higher level of protection than its physical counterpart? Worse, why should a criminal escape detection merely because she decides to digitize illegal material? Does this not set up a reverse incentive?

Child pornography, nuclear weapon designs, and counterfeit currencies, for instance, are all expressly forbidden under customs laws.[245] Why should the fact that a traveler carries them on an electronic device, instead of physically transporting a three dimensional representation, require the government to take additional steps to intercept it prior to importation? The materials encapsulate the same illegal behavior or threats. Shouldn't there be a way to foreclose a digital end-run around the customs regime? By not allowing officials to access the cloud, there is a real risk that travelers can simply transfer contraband from their devices to the cloud prior to entering the U.S., only to later download it within domestic borders.

The strongest response to the equivalence argument centers on the search, similarly considering the function of the search in the contemporary context. It

---

244. *See* Donohue, *supra* note 113.

245. *See, e.g.*, 19 U.S.C. § 1583(a)(1), (2) (2018) (empowering customs officials to engage in warrantless searches of international mail in relation to 18 U.S.C. §§ 1461, 1463, 1465, and 1466, which relate to obscenity and child pornography); *id.* at § 1583(d) (exempting from inspection sealed mail weighing less than 16 ounces); *id.* at § 1583(c)(1)(F) (empowering customs officials to search outgoing mail weighing in excess of 16 ounces sealed against inspection where there is reasonable cause to suspect that such mail contains child pornography); 6 U.S.C. § 211(c)(2) (2018) (tasking the Commissioner of U.S. Customs and Border Protection with ensuring "the interdiction of persons and goods illegally entering or existing the United States"); *id.* at § 211(c)(5) (requiring the commissioner to "detect, respond to, and interdict terrorists . . . and other persons who may undermine the security of the United States"); *id.* at § 211(c)(6) (requiring the commissioner to "safeguard the borders of the United States to protect against the entry of dangerous goods"); *see also* 18 U.S.C. § 2252(a)(1) (2018) (prohibiting the knowing international transportation or shipment of child pornography); *id.* § 2252(a)(2) (prohibiting receipt or distribution of child pornography); *id.* § 2252(4) (outlawing possession of child pornography); 19 U.S.C. § 1583(c)(1)(A) (providing for the examination of outbound mail); 31 U.S.C. § 5316 (2018) (requiring the reporting of the export and import of certain monetary instruments).

is not just digital contraband that is at stake once the Court allows the government to examine the mobile device or, through it, material held online. It is the traveler's entire life, as well as significant amounts of others' private affairs. It therefore is at once both intensely personal (as applied to that person and her family, friends, and acquaintances), and intrusive. While the search of a backpack, luggage, or shipping container might also reveal certain private matters, it does not in the process transmit the *whole* of a person's life.

To the extent that electronic searches reveal information that would otherwise be held in the home, moreover, historic protections drop away, steadily narrowing rights. Email has replaced letter correspondence, electronic calendars now take the place of planners, and the contacts list now serves as a telephone book. The border exception, applied to electronic devices, threatens to swallow protections which, for centuries, have limited government power.

An approach that takes into account the broader context of the search performed on the digital device dovetails with Fourth Amendment jurisprudence. The Court regularly applies a totality-of-the-circumstances analysis to probable cause determinations.[246] It uses it to determine reasonable suspicion.[247] And it employs it to ascertain voluntariness in granting consent to search.[248] In regard to electronic devices at the border, digital searches in which swathes of information becomes subject to government inspection changes the quality of the search itself. It is not the equivalent of looking in someone's luggage.

The Court has already taken this position in regard to the search of electronic devices *within* U.S. borders. In *Riley*, it held that the government could not search a mobile phone incident to arrest because the quality of the search itself was different.[249] The Court explained: "Cell phones . . . place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to . . . physical search."[250]

---

246. *See* Illinois v. Gates, 462 U.S. 213, 233, 238-39 (1983) (reaffirming "the "totality-of-the-circumstances" analysis that traditionally has informed probable cause determinations); *see also* Locke v. United States, 11 U.S. (7 Cranch) 339, 348 (1813) ("[T]he term 'probable cause,' according to its usual acceptation . . . imports a seizure made under circumstances which warrant suspicion.").

247. United States v. Arvizu, 534 U.S. 266, 273 (2002) ("When discussing how reviewing courts should make reasonable-suspicion determinations, we have said repeatedly that they must look at the 'totality of the circumstances' of each case to see whether the detaining officer has a 'particularized and objective basis' for suspecting legal wrongdoing.'").

248. Schneckloth v. Bustamonte, 412 U.S. 218, 227 (1973) ("[W]hether a consent to a search was in fact 'voluntary' or was the product of duress or coercion, express or implied, is a question of fact to be determined from the totality of all the circumstances.").

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

250. *Id.*

Because of this, the Court held that officers generally would be required to obtain a warrant.[251]

This also is the approach the Court has adopted regarding the border search exception writ large: the government cannot use the exception physically to search for undutied goods, contraband, and illegal entrants located on private property precisely because of the heightened privacy interests at stake. The founders were well aware of the dangers of allowing the government untrammeled access to individuals' lives. The border exception was therefore tailored to the country's sovereign interests in revenue generation and admitting qualified aliens, but it did not permit searches that went further afield.

And what of the end-run around customs by separating digital contraband from a particular traveler—for instance, by uploading it to the cloud, only to subsequently download it inside U.S. borders? Should Customs be able to access this information through the devices carried across international frontiers, potentially forcing the owners or users to provide passwords?

The first point to raise in response is that in-person physical transit has never been required for illegal goods to enter the country. The closest analogue would be use of the postal system. But as this Essay has explained, protections have been extended to the mail. A basic level of suspicion must be met to open sealed envelopes or packages of certain sizes.

A second point addresses the cloud concern: in a digital era, it is not only at ports of entry that the government has the opportunity to intercept digital contraband. Numerous laws, predicated on some level of individualized suspicion, provide an alternative means to access such materials. Law enforcement has the power to intercept wire, oral, and electronic communications related to a broad range of offenses, including *all* of those of interest to customs.[252] For stored communications, the government can obtain a

---

251. *Id.*

252. *See, e.g.*, 18 U.S.C. § 2516(a) (2018) (including any offense punishable by death or by imprisonment for more than one year related to enforcement of the Atomic Energy Act of 1954, the sabotage of nuclear facilities or fuel, espionage, kidnapping, treason, malicious mischief, the destruction of vessels, or piracy); *id* § 2516(b) (relating to murder, kidnapping, robbery, or extortion); *id* § 2516(c) (relating to, among others, violence at international airports, animal enterprise terrorism, arson, bribery, use of explosives, concealment of assets, transmission of wagering information, nuclear and weapons of mass destruction threats, explosive materials, loan and credit applications, protection of foreign officials, witness tampering, obstruction of criminal investigations, human trafficking, presidential staff, assassination, kidnapping, assault, interstate and foreign travel or violence linked to racketeering, theft, fraud, sexual exploitation of children, child pornography, stolen property, destruction of aircraft or aircraft facilities, mail fraud, computer fraud and abuse, nuclear material transactions, conspiracy, reproduction of naturalization or citizenship papers or passports, or forgery); *id* at § 2516(d) (counterfeiting); *id* at § 2516(g) (relating to currency transactions).

court order based on "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[253] The order can be served on electronic communication or remote computing services.[254] The government can also obtain stored communications 180 days old (or less) via a warrant.[255] In 2016, changes to Rule 41 enabled agencies to obtain a warrant for remote access search and seizure of digital information.[256]

Foreign intelligence surveillance authorities also play a role in addressing international criminal conspiracies. In light of post-9/11 changes to the Foreign Intelligence Surveillance Act,[257] and the infamous demise of the wall between foreign intelligence and criminal investigations, foreign intelligence laws are used to monitor international threats, even when the primary purpose of surveillance is criminal in nature.[258] To the extent that provisions like the FISA Amendments Act do not apply, collection techniques consistent with Executive Order 12,333 may.[259] In the context of non-U.S. persons, the government has even broader authorities.[260]

For digital data, as a matter of constitutional law, increasingly stringent requirements must be met for more invasive searches Because of the nature of electronic devices, no search can take place without, at a minimum, reasonable suspicion. The types of crimes to which such searches can be directed are only those explicitly authorized by Congress—not general criminal activity. For more invasive searches, probable cause and a warrant are required. Even here, the search must be appropriately circumscribed to avoid the type of general warrants prohibited by the Fourth Amendment.

---

253. 18 U.S.C. § 2703(d).

254. *Id.* § 2703(b), (c).

255. *Id.* § 2703(a).

256. FED. R. CRIM. P. 41.

257. *See* Foreign Intelligence Surveillance Act of 1979 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

258. *See* Laura K. Donohue, Bulk Metadata Collection: Statutory and Constitutional Considerations, 37 HARV. J.L. & PUB. POL'Y 757 (2014).

259. Exec. Order 12,333, 3 C.F.R. § 200 (1982), *reprinted as amended in* 50 U.S.C. § 3001 app. at 418-27 (2013).

260. *See generally* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015); *The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law,* COUNCIL ON FOREIGN REL. (June 26, 2017), https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law [https://perma.cc/U39E-JPF5].

B. Immigration

A second major challenge to this Essay's argument could be raised regarding immigration. One might argue that part of the reason the government subjects noncitizens to searches prior to entering the United States is to ascertain whether they are who they purport to be, and what sorts of individuals are being admitted to the country. Surely, the type of information present in travelers' electronic devices is relevant to such a determination. It could be considered irresponsible not to look at social media or the full range of an individual's background—particularly where U.S. national security is on the line. Certainly, the powers of sovereignty undergirding the border exception provide adequate room for such examinations.

This is a strong argument. However, *it does not apply to U.S. persons.* Once a traveler establishes her identity as a citizen or legal resident, if there are no arrest alerts or other warrant notifications tied to the passport, there is *no* reason, under traditional immigration provisions, to commence a search. This is a bright-line rule. Probable cause must exist for a search of the person and, even then, it must meet the particularity required in the second clause of the Fourth Amendment.

The challenge thus applies solely to aliens. Here, as a constitutional matter, the government has more latitude than with regard to U.S. persons. Part of the function of the immigration services is to ascertain whether aliens admitted to the United States—either as visitors or as potential citizens—meet the policies set by Congress. As Chief Justice Rehnquist noted in *Verdugo-Urquidez*, a non-U.S. person lacking a substantial connection to the United States does not enjoy Fourth Amendment protections. To the extent, then, that the executive seeks to build profiles of non-U.S. persons entering or leaving the United States, the question appears primarily to be one of policy and statute, not one of constitutional law.

Nevertheless, as a constitutional matter, as well as an historical one, it remains for *Congress*, not the executive branch, to make this determination. An additional policy consideration is worth noting: in granting visitors access to the United States, the point at which background material would be most relevant is at the point at which a visa issues (at least for countries for which a visa is required). This suggests reviewing material at an earlier point in time, instead of focusing on the border crossing as an opportunity to look more carefully at those entering and leaving the United States. Whether or not this is a good idea in terms of the effect on U.S. foreign relations, or how U.S. citizens are treated in other countries, is a policy question. The decision of who and what to search, as applied to non-U.S. persons requires that Congress carefully consider myriad competing interests.

CONCLUSION

Many cases challenging the constitutionality of searches of electronic devices are beginning to move through the courts.[261] In light of the significant Fourth Amendment issues at stake, this Essay has endeavored to explain the origins and evolution of the border search exception, which is justified only by its narrow purpose: the interdiction of contraband and the regulation of noncitizens entering the United States. In the process, it has argued that the *nature* of digitized searches differs in important respects from physical ones. Thus, while the transportation of digital contraband is still illegal, if the border search exception applies to electronic devices, the government's use of it may be so broad as to render the Fourth Amendment obsolete. There is a reason that, in the past, the government was limited by geography and time, by the manner of transportation, the size of the item being inspected, the agency allowed to conduct the inspection, and the crimes for which they could interdict persons or materials. There are currently few, if any, equivalent border restrictions for digital contraband. Yet numerous alternative statutory instruments would allow for the interdiction of such materials.

As a matter of immigration law, as soon as a traveler establishes her identity as a U.S. citizen, the government must have probable cause, supported by a sufficiently particularized warrant, to search her electronic devices. Non-U.S. citizens lacking a substantial connection to the country are in a different constitutional category. Here, because of significant policy concerns, and Congress's historic authority over immigration, the legislature has an important role to play. What is needed now, particularly post-*Riley*, *Jones*, and *Carpenter*, is a more careful approach, grounded in reasonable suspicion and probable cause, that is cognizant of the significant constitutional issues at stake in the inspection of travelers' electronic devices.

---

261. *See, e.g.*, Abidor v. Napolitano, 990 F. Supp. 2d 260, 267, 268 (E.D.N.Y. 2013) (challenging a search of a dual U.S./French citizen at the Canadian border in which the traveler's laptop was searched, confiscated, and returned after eleven days with evidence that his personal files—including his research, photos, and chat history with his girlfriend—had been searched); Alasaad v. Nielsen, No. 17-CV-11730-DJC, 2018 WL 2170323 (D. Mass. May 9, 2018); Complaint at 1, Alasaad v. Duke, 1:17-CV-11730-DJC (D. Mass. Sept. 13, 2017) (challenging search and seizure of smartphones, laptop, and other electronic devices at the U.S. border in violation of the First and Fourth Amendments); *see also* Daniel Victor, *Forced Searches of Phones and Laptops at U.S. Border Are Illegal, Lawsuit Claims*, N.Y. TIMES (Sept. 13, 2017), https://www.nytimes.com/2017/09/13/technology/aclu-border-patrol-lawsuit.html [https://perma.cc/PAK4-47KU]; Deb Riechmann, *Are Searches of Laptops and Cellphones by Border Agents Unconstitutional?*, PBS (Sept. 13, 2017), http://www.pbs.org/newshour/rundown/searches-laptops-cellphones-border-agents-unconstitutional [https://perma.cc/58HW-G7J4].

Professor of Law, Georgetown Law. *Special thanks to Jeremy McCabe at the Georgetown Law Library, who helped to obtain a number of the primary sources addressed in this Essay, as well as Grant Tanenbaum, for his research assistance. Professor Orin Kerr kindly provided comments. An early draft of this Essay was submitted, with the permission of the editors of* Yale Law Journal*, as written testimony to the U.S. Senate Committee on Homeland Security and Government Affairs' Subcommittee on Federal Spending Oversight and Emergency Management.* Hearing to Examine Warrantless Smartphone Searches at the Border: Hearing Before the Subcomm. on Fed. Spending Oversight & Emergency Mgmt. of the S. Comm. on Homeland Sec. & Governmental Affairs, *115th Cong. (2018) (statement of Laura K. Donohue)*.