CAN WE CURATE IT? WHY LUGGAGE AND SMARTPHONES MERIT DIFFERENT TREATMENT AT THE UNITED STATES BORDER

Maddalena DeSimone*

The Fourth Amendment protects against unreasonable searches and seizures. At the United States border, however, sovereignty interests—namely who and what enters the country—allow for warrantless searches of property without probable cause. This Note explores the reach of the border exception to one category of property: electronic devices. At present, circuit courts disagree over what level of suspicion—no suspicion or reasonable suspicion—applies to forensic searches of electronics. Courts do agree that manual searches, performed without the assistance of external equipment, merit no suspicion at all. The suspicion gap between manual and forensic searches reflects an assumption that all manual searches are cursory and hence violate a device owner's privacy less than a forensic search.

This Note argues that the existing line between forensic and manual searches should be reimagined; instead, electronic devices, such as smartphones, should be separated out from other electronic devices, such as cameras, and be subject to a reasonable suspicion standard irrespective of the nature of the search, forensic or manual. Redrawing the line between devices themselves recognizes that certain electronics (e.g. cameras) are more analogous to traditional luggage and therefore should receive the same treatment at the border where suspicionless searches are permitted. Like luggage, one can curate these devices: it is possible to know

* J.D. Candidate 2020, Columbia Law School; B.A. 2013, College of William & Mary. Many thanks to Professor Tim Wu for his thoughtful comments on content and my sincerest gratitude to the staff and editorial board of the *Columbia Business Law Review* for their dedication and attention to detail in preparing this Note for publication.

and choose what is inside. As the attenuation of the link between the device in question and traditional luggage expands, so too should the suspicion required. Smartphones and like devices should not be searched without reasonable suspicion. Finally, this Note concludes by recommending that the Customs and Border Protection directive, subject to review and modification every three years, be revised to distinguish between the two groups of electronic devices and account for the privacy concerns unique to the smartphone and related devices group.

I. INTRODUCTION

> Remove the 3-1-1 liquids bag and place it in the bin. Ensure pockets are empty (keys, tissues, currency, wallets, cell phones, etc.) and remove bulky jewelry (valuable items can be placed in carry-on). Remove your shoes and place them directly on the X-ray belt. Remove personal electronic devices larger than a cell phone from your carry-on bag and place them into a bin with nothing placed on or under them for X-ray screening (E.g. laptops, tablets, e-readers and handheld game consoles). Remember to check the bins and collect all belongings after going through screening.[1]

Anyone who travels is familiar with this routine. X-ray screening of cell phones, laptops, and iPads is standard procedure at the airport.[2] However, people are less familiar with secondary manual and forensic searches of electronics.[3] The U.S. Customs and Border Protection ("CBP") defines a manual or "basic search" as an examination of an electronic device by an officer with the possibility of review and analysis

---

[1] *Travel Checklist*, TRANSP. SECURITY ADMIN., https://www.tsa.gov/travel/travel-tips/travel-checklist [https://perma.cc/C45H-P7RB].

[2] *See* Michelle Higgins, *Security Ahead? Pack Patience*, N.Y. TIMES (Jan. 19, 2010), https://www.nytimes.com/2010/01/24/travel/24pracsecurity.html [https://perma.cc/9CW5-UWBC].

[3] *See generally* Derek Hawkins, *The Cybersecurity 202: Warrantless Device Searches at the Border are Rising. Privacy Advocates are Suing*, WASH. POST (Aug. 7, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/08/07/the-cybersecurity-202-warrantless-device-searches-at-the-border-are-rising-privacy-advocates-are-suing/5b6883771b326b0207955f46/?noredirect=on&utm_term=.12bfa38d02ac [https://perma.cc/MS9Q-CV9Y].

of information encountered at the border.[4] In other words, this includes opening and scrolling-through a cell phone's contents, including call history, text messages, photos, apps—such as WhatsApp or Facebook Messenger—and social media accounts.[5] A forensic search or "advanced search" is defined as "any search in which an Officer connects external equipment . . . not merely to gain access to the device, but to review, copy, and/or analyze its contents."[6] A forensic search is not an action to determine if a device functions, to determine if the device conceals physical contraband within, or to review information voluntarily provided in electronic format, such as an airline e-ticket.[7] Additionally, it is limited to data found on the physical device at the time of travel.[8] Consequently, data stored on the cloud is exempt from search.[9]

In 2016, CBP searched the electronic devices of 19,051 international travelers, both inbound and outbound.[10] The

4 *See* U.S. CUSTOMS & BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES § 5.1.3 (2018) [hereinafter CBP DIRECTIVE], 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/Z389-P2M7].

5 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/35JM-XRH8]. While a border agent cannot force an individual to unlock a password protected device, she may seize the device if someone refuses to do so. *See id.*

6 CBP DIRECTIVE, *supra* note 4, § 5.1.4.

7 *See id.* § 2.3.

8 *Id.* § 5.1.2.

9 *See id.*; *see also* CBP DIRECTIVE, *supra* note 4, § 5.1.2; Brian Fung, *Travelers Just Won Back a Bit of Their Privacy at the Border*, WASH. POST (July 14, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/07/14/travelers-just-won-back-a-bit-of-their-privacy-at-the-border/ [https://perma.cc/PM2U-WRZN].

10 Press Release, U.S. Customs & Border Prot., CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and [https://perma.cc/Y6CG-VHFM].

following year, CBP reported 30,200 international travelers had their electronics searched, an increase of almost sixty percent from 2016.[11] Such searches are likely to continue to climb given the unprecedented rise in electronics use[12] and the sustained popularity of the United States as a travel destination.[13] Put briefly, CBP officials are likely to increasingly scrutinize international travelers' essential electronics.[14]

According to the CBP's January 2018 directive, which is up for review in January 2021, the searches are "essential to enforcing law at the U.S. border and to protecting border security."[15] They assist in detecting evidence related to terrorism, human and bulk cash smuggling, contraband, and child pornography.[16] The searches also seek to expose

[11] *Id.*

[12] Ninety-five percent of Americans now own a cell phone. *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/Q9YJ-9NU8]. Seventy-seven percent have a smartphone, a spike from thirty-five percent in 2011. *Id.* Non-cell phone electronics use is also climbing; nearly three quarters of American adults now own desktop or laptop computers, over one-half own tablet computers, and about one-fifth own e-reader devices. *Id.* (showing that seventy-three percent of U.S. adults own desktop/laptop computers and fifty-three percent own tablets, as of January 10, 2018, and that twenty-two percent own e-readers as of November 6, 2016).

[13] The United States remains a popular travel choice, as the largest destination for global long-haul travel and third-largest destination for overall global travel. *Fact Sheet: International Inbound Travel to the U.S. (2017)*, U.S. TRAVEL ASS'N, https://www.ustravel.org/system/files/media_root/document/Research_Fact-Sheet_International-Inbound.pdf [https://perma.cc/9K3F-DRAG] (last updated Oct. 2018). Global long-haul travel is travel between countries from separate geographical regions (e.g. between the United States and Germany) and excludes inter-regional travel (e.g. between the U.S. and Canada). *Id.* The United States welcomed an unprecedented 75.9 million international visitors in 2016. OECD, OECD TOURISM TRENDS AND POLICIES 2018 (2018), https://www.oecd-ilibrary.org/sites/tour-2018-en/table-103.html?itemId=/content/component/tour-2018-table103-en [https://perma.cc/E2YJ-M3YW].

[14] *See* Hawkins, *supra* note 3.

[15] CBP DIRECTIVE, *supra* note 4, § 1.

[16] *Id.* Searching such devices can improve risk assessments of individual travelers and information sharing with the federal government

information about financial and commercial crimes, including those involving copyright, trademark, and export control violations.[17] While these searches have many purported security benefits, they also raise privacy concerns for a number of stakeholders who share an interest in the electronics of their data.[18] While the vast majority of persons searched are international visitors,[19] this Note focuses on the constitutional protections of citizens and permanent legal residents. Although device owners' privacy interests are underscored first and foremost, third parties such as business entities are also implicated. Company trade secrets or intellectual property could be at risk when employees leave the country on business.[20] Furthermore, business personnel

responsible for analyzing terrorist threats. *Id.* CBP claims that the searches are "integral to a determination of an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws." *Id.*

17 *Id.*

18 One case particularly exemplifies the diversity of individuals subject to search. In *Alasaad v. Nielson*, plaintiffs included an artist, an employee of NASA's Jet Propulsion Laboratory, journalists from Massachusetts and Virginia, a New York filmmaker, and a college professor and former captain of the U.S. Air Force from Florida. *See* Alasaad v. Nielsen, No. 17-CV-11730, 2018 WL 2170323, at *5–8 (D. Mass. May 9, 2018).

19 A senior CBP official reported that approximately twenty percent of travelers whose devices are inspected are U.S. citizens. Nick Miroff, *U.S. Customs Agents Are Searching More Cellphones – Including Those Belonging to Americans*, WASH. POST (Jan. 5, 2018), https://www.washingtonpost.com/world/national-security/us-customs-agents-are-searching-more-cellphones--including-those-belonging-to-americans/2018/01/05/0a236202-f247-11e7-b3bf-ab90a706e175_story.html?noredirect=on&utm_term=.9cf112c67631[https://perma.cc/7NE6-D4Y2].

20 *See* Sara H. Jodka, *If You Don't Need It, Don't Pack It: Border Searches of Mobile Devices*, NAT'L L. REV. (Mar. 21, 2018), https://www.natlawreview.com/article/if-you-don-t-need-it-don-t-pack-it-border-searches-mobile-devices [https://perma.cc/CW83-5FCW]; *see also* Daniel R. Levy, *It's a Brave New World: Protecting Trade Secrets When Traveling Abroad with Electronic Devices*, TRADE SECRETS & EMP. MOBILITY (Feb. 13, 2018), https://www.tradesecretsandemployeemobility.com/2018/02/articles/trade-secrets-and-confidential-information/its-a-brave-new-world-protecting-trade-secrets-when-traveling-abroad-with-electronic-devices/ [https://perma.cc/K8TH-PU8A].

may travel with electronics that do not belong to them, but to their employer.[21]

These weighty privacy considerations are prompting some individuals to turn to the courts for guidance.[22] Federal judges across the United States are wrestling with the tension between national security and privacy.[23] Currently, all circuit courts agree that no suspicion is required for manual searches.[24] They split, however, over what level of suspicion is required for forensic searches, no suspicion or reasonable suspicion.[25] This Note reimagines the line drawn between manual and forensic searches and instead argues for a new divide between types of electronic devices, with less suspicion required for fully curated[26] devices that are most analogous to traditional luggage.

Part II of this Note traces the origins of the Fourth Amendment right against unlawful search and seizure and the birth of the border exception, and introduces the Supreme Court's holdings on cell phone searches outside of the border context in *United States v. Riley*[27] and *United States v.*

21 *See* Thomas Lonardo, Doug White, Tricia P. Martland & Alan Rea, *Legal Issues Regarding Digital Forensic Examiners Third Party Consent to Search*, 6 J. DIGITAL FORENSICS, SECURITY & L., no. 4, 2011, at 19, 22. In such cases where sensitive business documents are found, the CBP directive instructs its officers to "treat such information as business confidential information and . . . protect that information from unauthorized disclosure." CBP DIRECTIVE, *supra* note 4, § 5.2.3. The directive recognizes that the Trade Secrets Act, the Privacy Act, and other laws and CBP policies may inform the handling of such information. *Id.*

22 *See Alasaad*, No. 17-CV-11730, 2018 WL 2170323, at *1 (listing ten U.S. citizens and one lawful permanent resident whose devices were searched at U.S. ports of entry and have subsequently sought declaratory and injunctive relief).

23 *See, e.g.*, United States v. Kolsuz, 890 F.3d 133, 150 (4th Cir. 2018) (Wilkinson, J., concurring) (listing questions which add color to this tension at the border).

24 *See infra* Section III.A.1.

25 *See infra* Part III.

26 Just as a suitcase is curated, in the sense that the owner chooses what she does and does not wish to pack, so too are certain electronic devices. *See infra* Section V.B.2.

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

Carpenter.[28] Part III examines the existing circuit split over the level of suspicion required for forensic searches of electronic travel items. Part IV revisits the border exception and suggests a partial untethering of government interests in favor of individuals' privacy interests in smartphones. Finally, Part V agrees with the Fourth and Ninth Circuits' requirements[29] of at least reasonable suspicion for forensic searches of smartphones and laptops, but proposes that the type of device, not the type of search (manual or forensic) should inform the level of suspicion required. Specifically, this Note argues that searches of devices that are curated—such as digital cameras—should be exempt from any enhanced suspicion, but searches of devices that are not fully curated—such as smartphones—should be subject to a reasonable suspicion standard.

II. THE FOURTH AMENDMENT AND UNREASONABLE SEARCHES AND SEIZURES

A. *Katz* and the Reasonable Expectation Standard

The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[30]

In *Katz v. United States*, the Supreme Court stated that these Fourth Amendment protections applied to "people not places."[31] But what right to protection are people entitled to?

---

[28] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[29] For a full discussion of these requirements, see *infra* Part V.

[30] U.S. CONST. amend. IV.

[31] Katz v. United States, 389 U.S. 347, 351 (1967) (holding that the government's eavesdropping and recording of a man's spoken words in a public telephone booth constituted an unreasonable search and seizure, not

The Court cautioned that the Amendment is not a "general constitutional right to privacy."[32] Instead, it protects against *certain* governmental intrusions, while leaving any protection for a person's general right to be left alone to the individual states.[33] While "people, not places" are protected, courts examine references to specific places to determine whether a person is afforded protection from particularized governmental intrusion.[34] In his concurring opinion in *Katz*, Justice Harlan articulated a two-step test that the Supreme Court has since adopted as governing law.[35] To determine whether a Fourth Amendment violation has occurred, the Court engages in an inquiry that is both subjective and objective. First, the person must possess an "actual (subjective) expectation of privacy."[36] Second, that expectation must "be one that society is prepared to recognize as 'reasonable.'"[37]

Justice Harlan's two-fold requirement in *Katz* has been echoed in the Supreme Court's recent holding in *Carpenter v. United States*: "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' . . . official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause."[38] However, the *Katz* test for legitimate expectations of privacy supplements "'the traditional property-based

due to location alone, but because of his justifiable reliance upon privacy therein).

[32] *Id.* at 350 (internal quotation marks omitted).

[33] *Id.* at 350–51.

[34] *Id.* at 361 (Harlan, J., concurring).

[35] *See* Byrd v. United States, 138 S. Ct. 1518, 1526 (2018); *see also* Kyllo v. United States, 533 U.S. 27, 33 (2001).

[36] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[37] *Id.* For example, in the case of the telephone booth in *Katz*, the defendant's expectation was "reasonable" because of the nature of the booth: When it is occupied, the caller closes the door and may assume that the conversation is not overheard. *Id.* at 361.

[38] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)).

understanding of the Fourth Amendment.'"[39] Historically, the doctrine was "tied to common-law trespass"[40] and guarded against the Government "obtain[ing] information by physically intruding on a constitutionally protected area[.]"[41] During colonial times, general warrants and writs of assistance permitted British officers to forage through homes in pursuit of evidence of criminal activity.[42] The Fourth Amendment's plain language—"houses, papers, and effects"[43]—clearly demonstrates the Framers' resolve to protect certain forms of tangible property, especially those found in the sanctity of one's home, from the Government's "arbitrary power"[44] and "a too permeating police surveillance."[45]

The Supreme Court has found reasonable expectations of privacy in a number of sub-spheres: car ownership and possession;[46] buses;[47] cell phone records;[48] burned buildings;[49] and porches,[50] among others. Even without a

[39] *Byrd*, 138 S. Ct. at 1526 (citing Florida v. Jardines, 569 U.S. 1, 11 (2013)).

[40] United States v. Jones, 565 U.S. 400, 405 (2012).

[41] *Id.* at 406 n.3 (2012).

[42] *See* Riley v. California, 573 U.S. 373, 403 (2014).

[43] U.S. CONST. amend. IV.

[44] Boyd v. United States, 116 U.S. 616, 630 (1886).

[45] United States v. Di Re, 332 U.S. 581, 595 (1948).

[46] *See* Byrd v. United States, 138 S. Ct. 1518, 1527 (2018) (holding that a driver in lawful possession or control of a rental car, yet not listed as an authorized driver on the rental agreement, retains her otherwise reasonable expectation of privacy under the Fourth Amendment). Note that mobile homes are afforded less protection under the Fourth Amendment because they are readily movable before the execution of a warrant. *See* California v. Carney, 471 U.S. 386, 393 (1985).

[47] *See* Bond v. United States, 529 U.S. 334, 335 (2000) (holding that a bus passenger's privacy expectation for his carry-on bag was reasonable).

[48] *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (holding that a seizure and search of cell phone records revealing location and movements of a user over the course of 127 days required a warrant).

[49] *See* Michigan v. Clifford, 464 U.S. 287, 297 (1984) (holding that reasonable expectations of privacy may be found in fire-damaged premises).

[50] *See* Florida v. Jardines, 569 U.S. 1, 6 (2013) (finding that the front porch of a home is part of the home itself and not subject to warrantless

recognized common law property interest in the place searched, a person may nonetheless claim a reasonable expectation of privacy in it.[51] In doing so, however, she must claim more than a mere legitimate presence on the premises searched.[52] Presence without more "creates too broad a gauge for measurement of Fourth Amendment rights."[53] The Court illustrated this point with two hypotheticals in *Rakas v. Illinois*: first, a visitor not welcome in a specified area of her host's home that is searched (e.g., the basement) and second, a visitor who enters the host's home one minute before the search and leaves one minute after.[54] In both scenarios, the visitor has no legitimate expectation of privacy in the premises.

Assuming a valid and reasonable expectation of privacy exists, "no [w]arrants shall issue but upon probable cause."[55] While the Fourth Amendment does not elaborate further, in *Illinois v. Gates*, the Supreme Court employed a practical, non-technical, totality-of-the-circumstances standard consistent with probabilities inherent in the "factual and practical considerations of everyday life on which reasonable and prudent men . . . act."[56] In the context of searches, probable cause exists when "there is a fair probability that contraband or evidence of a crime will be found in a particular

investigation by drug-sniffing dogs). In her concurring opinion, Justice Elena Kagan added that people have a heightened expectation of privacy not only within their homes, but in also in areas immediately surrounding their homes. *Id.* at 13 (Kagan, J., concurring). The Court, by contrast, has declined to find reasonable expectations of privacy in areas above homes, such as airspace. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 215 (1986); *see also* Florida v. Riley, 488 U.S. 445, 445 (1989).

51 *See, e.g.*, *Byrd*, 138 S. Ct. at 1527 (citing Jones v. United States, 362 U.S. 257, 259 (1960); Katz v. United States, 389 U.S. 347, 352 (1967); Mancusi v. DeForte, 392 U.S. 364, 368 (1968); Minnesota v. Olson, 495 U.S. 91, 98 (1990)).

52 *See* Rakas v. Illinois, 439 U.S. 128, 147–48 (1978).

53 *Id.* at 142.

54 *See id.*

55 U.S. CONST. amend. IV.

56 Illinois v. Gates, 462 U.S. 213, 231 (1983).

place."[57] When issuing a warrant, the magistrate judge relies on all the circumstances set forth in the affidavit before her, including the credibility of hearsay information provided.[58] Bare conclusory statements are insufficient.[59] For example, a sworn statement that affiant "has cause to suspect and does believe that" illegal liquor is located on the premises does not pass muster.[60] In *Gates*, however, an anonymous letter regarding defendant's illicit drug activities, corroborated in part by federal agents, sufficed to meet probable cause.[61]

B. Warrantless Search of Electronics

As electronics ownership has become virtually ubiquitous,[62] the law surrounding reasonable electronics searches gains salience. The Supreme Court required warrants issued upon probable cause for unreasonable searches of electronics in two landmark cases.[63]

First, in 2014, the Court held that a warrantless search and seizure of cell phone contents during an arrest generally violates the Fourth Amendment.[64] *Riley v. California* consolidated two cases, the first of which involved a man arrested on weapons charges whose pockets were searched and cell phone seized incident to the arrest.[65] The officer who seized Riley's phone noticed the repeated use of a term associated with a street gang.[66] Two hours later, a detective further examined the phone at the police station and found photographs and videos providing at least partial basis for

57 *Id.* at 238.

58 *See id.*

59 *See id.* at 239.

60 *See* Nathanson v. United States, 290 U.S. 41, 44, 47 (1933).

61 *See Gates*, 462 U.S. at 243.

62 *See Mobile Fact Sheet*, *supra* note 12.

63 *See* Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373 (2014).

64 *Riley*, 573 U.S. at 386.

65 *Id.* at 378–79.

66 *Id.* at 379.

subsequent charges in connection with a shooting that occurred a few weeks prior.[67]

The Court stated that "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the [Fourth Amendment's] warrant requirement."[68] A warrantless search incident to lawful arrest is one such exception.[69] The lawful arrest, however, is limited by certain conditions. The Court cited the foundational search-incident-to-arrest case, *Chimel v. California*, for the requirement that a search of an area within the arrestees "immediate control" either (1) promotes officer safety or (2) preserves evidence.[70] The Court, however, distinguished the search of cell phones, finding that the digital data stored on them presented neither of the two *Chimel* risks: It cannot itself be used as a weapon to harm an officer, and remote-wiping may be fully prevented by disconnecting a phone from its network.[71] Moreover, the Court rejected the government's assertion that a search of cell phone data is "materially indistinguishable" from similar searches of physical items: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[72] Both are means of getting from point A to point B, but, beyond that, do not belong together. The Court further explained that categorically, modern cell phones implicate

67 *Id.* Riley was ultimately charged with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder. *Id.* The jury convicted him of all three counts and the trial court sentenced him to fifteen years to life in prison, an enhanced sentence based on the aggravating factor of committing crimes for the benefit of a street gang. *Id.* at 380.

68 *Id.* at 382 (citing Kentucky v. King, 181 S. Ct. 1849, 1856–57 (2011)).

69 *Id.* The Court points to Weeks v. United States, 232 U.S. 383 (1914), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961), as the case that first recognized the government's right to search arrestees without a warrant.

70 *Id.* at 382–83 (citing Chimel v. California, 395 U.S. 752, 762–63 (1969), *abrogated on other grounds by* Davis v. United States, 564 U.S. 229 (2011)). The Court in *Chimel* found a warrantless search of man's entire house incident to proper arrest to be unlawful because it was beyond his person or the area where incriminating evidence could be found. *Chimel*, 395 U.S. at 768.

71 *Riley*, 573 U.S. at 386–90.

72 *Id.* at 393.

privacy concerns that surpass those attached to a cigarette pack or wallet, items traditionally seized post-arrest.[73] It cautioned against relying too heavily on the term "cell phone," likening them instead to minicomputers with telephone capacity.[74] To support the Court's hard line drawing, it cited cell phones' storage capacity, a unique element of pervasiveness, and qualitative differences, such as browsing history.[75]

Four years later, the Supreme Court revisited cell phones in a different context: cell-site records. One function that cell phones perform is continuous connection to a set of radio antennas or cell sites.[76] When a cell phone connects to such a site, it leaves behind a time stamped record.[77] These records are collected and stored by wireless carriers for business purposes.[78]

In *United States v. Carpenter*, prosecutors were granted court orders to obtain cell phone records of robbery suspects identified by the FBI pursuant to the Stored Communications Act.[79] The wireless carrier's production revealed 12,898 location points cataloging defendant Timothy Carpenter's movements over 127 days.[80] Carpenter moved to suppress the data, claiming that use of the location points was an unconstitutional search under the Fourth Amendment.[81] The lower courts rejected his contention, finding no reasonable expectation of privacy because Carpenter shared his location data with his wireless carriers.[82]

---

[73] *Id.*

[74] *Id.*

[75] *Id.* at 393–95. For a further discussion of these arguments, see *infra* Section V.B.

[76] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

[77] *Id.* This record is known as cell-site location information. *Id.*

[78] *Id.* at 2212.

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.* at 2212–13. If one voluntarily shares or turns over information to a third-party, she loses a legitimate expectation of privacy in such information under the third-party doctrine. *Id.* at 2216 (citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

In its reversal, the Supreme Court discussed two lines of intersecting cases addressing a person's expectation of privacy: (1) in her physical location and movements, and (2) in information voluntarily turned over to third parties.[83] With respect to the first issue, the Court again stressed the one-of-a-kind nature of the digital data at issue. While rudimentary car tracking by beeper does not constitute a search,[84] the Court found the cell-site tracking here to be more closely aligned with the unconstitutional GPS tracking device used in *United States v. Jones*.[85] The second point reflected a common-sense doctrine, based on an understanding that one loses her expectation of privacy in information upon voluntarily sharing it with a third party. The Court applied this logic in the past to bank records in *United States v. Miller*[86] and outgoing phone numbers dialed on a landline telephone in *Smith v. Maryland*.[87] In *Carpenter*, however, the Court confronted a "new phenomenon"[88]—one in which the phone

[83] *Id.* at 2215–16.

[84] *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

[85] United States v. Jones, 565 U.S. 400 (2012). In *Jones*, FBI agents' installation of a GPS tracking device on Jones's vehicle and subsequent monitoring for twenty-eight days constituted an illegal trespass. *Id.* at 403–04, 412. While the case was decided on the basis of physical trespass, concurring justices recognized "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 430 (Alito, J., concurring).

[86] United States v. Miller, 425 U.S. 435, 442 (1976). In *Miller*, the Court held that the government's subpoena of Miller's bank records during a tax evasion investigation did not violate the Fourth Amendment. *Id.* at 445. Miller's checks, deposit slips, and monthly statements were not confidential communications because Miller used them in commercial transactions observed by bank employees in the ordinary course of business. *See id.* at 442.

[87] *See Smith*, 442 U.S. at 741, 743. Use of pen registers—devices that record the outgoing numbers dialed by a certain phone—did not constitute a search because telephone subscribers know that the numbers they dial are used by the telephone company for a variety of business reasons. *Id.* at 744.

[88] *Carpenter*, 138 S. Ct. at 2216.

and its user are inseparable, resulting in not merely a list of dialed digits, but a comprehensive constellation of a person's every movement. Put differently, the revealing nature of cell-site records is incomparable to bank checks or telephone call logs. Moreover, cell-site data is not "shared" in the traditional sense; the only affirmative act required on behalf of the user is to power on the device.[89] In sum, the Court held that the government's acquisition of Carpenter's cell-site records without a warrant supported by probable cause constituted a search in violation of the Fourth Amendment.[90]

C. The Border Exception

The Fourth Amendment protects against warrantless, unreasonable searches and seizures when travelling from one state into another within the continental United States.[91] But this protection recedes at the border, where warrantless searches of property without probable cause are permitted.[92] At the border, the sovereign's long-standing right to control "who and what may enter the country" reigns supreme, "subject to substantive limitations imposed by the Constitution[.]"[93] In *United States v. Flores-Montano*, the Supreme Court instructed that it is this very sovereign right that makes these searches "reasonable simply by virtue of the fact that they occur at the border."[94]

Several constitutionally enumerated powers underlie the government's border search authority: Congress' "'broad powers . . . to prevent smuggling and to prevent prohibited articles from entry,' under its plenary authority '[t]o lay and collect Taxes, Duties, Imposts and Excises,' '[t]o regulate Commerce with foreign Nations,' and '[t]o establish a [ ]

89 *See id.* at 2220.

90 *See id.* at 2221.

91 *See* Carroll v. United States, 267 U.S. 132, 154 (1925).

92 See *id.* at 153–54.

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

94 United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004) (quoting *Ramsey*, 431 U.S. at 616).

uniform Rule of Naturalization.'"[95] At the core of these exceptional powers, however, is the accepted premise that "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its *zenith* at the international border."[96] This interest is motivated by a need to protect United States citizens from "the introduction of contraband into this country"[97]—including child pornography or narcotics.

Some privacy rights, however, survive the border exception. Indeed, an individual's privacy rights are not usurped in their entirety, but "[b]alanced against the sovereign's interests."[98] While the Supreme Court has never required probable cause for searches at the border, the Court has applied this balancing test to extend a reasonable suspicion requirement to "highly intrusive searches of the person;" "searches of property [that] are . . . so destructive;" and searches conducted in "a particularly offensive manner."[99] Reasonable suspicion is a step below probable cause—it is less than a showing of a fair probability of criminal evidence, but more than a "hunch"[100] of criminal activity.

In *United States v. Montoya de Hernandez*, the Supreme Court held that prolonged detention of a traveler at the border is justified if customs officers "*reasonably suspect* that the traveler is smuggling contraband in her alimentary canal."[101] The traveler in this case, a Colombian woman travelling from Bogotá to Los Angeles, swallowed eighty-eight balloons of

95 United States v. Touset, 890 F.3d 1227, 1232 (11th Cir. 2018) (internal citations omitted).

96 *Flores-Montano*, 541 U.S. at 152 (emphasis added).

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

98 *Id.* at 539. This balance, however, is "struck much more favorably to the Government at the border." *Id.* at 540.

99 *Flores-Montano,* 541 U.S. at 152, 154 n.2, 156 (quotations omitted). The Court, however, failed to specify the circumstances under which a search would be considered unreasonable because it was conducted in a "particularly offensive manner." *Id.* at 154 n.2.

100 *Montoya de Hernandez*, 473 U.S. at 542.

101 *Id.* at 541 (emphasis added).

cocaine.[102] While the concern for the protection of the integrity of the United States border from the entry of unwanted narcotics is undeniable, a "particularized and objective basis for suspecting the [defendant]"[103] is nonetheless required to justify such an extreme invasion of personal privacy and dignity inherent in an alimentary canal search.[104]

The focal point of the Court's discussion, however, remains "reasonableness."[105] But what is reasonable at the border? The answer lies in the totality of the circumstances surrounding the search and the nature of the search itself.[106] Scope and duration of the privacy deprivation are but two factors in a larger calculus.[107] The starting line, however, is not evenly marked across the board. Because the government's legitimate interest at the border meets a traveler's diminished interest, the traveler's privacy deprivation must overcome the government's sovereignty-based advantage before it is considered unreasonable.

III. CIRCUIT SPLIT OVER LEVEL OF SUSPICION REQUIRED FOR FORENSIC SEARCHES

Section II.B discussed the Supreme Court's view on a warrant requirement for cell phone searches in two limited contexts: search-incident-to-arrest and cell-site records.[108] The Supreme Court, however, has yet to weigh in on such a requirement for border searches.[109] Instead, the various

[102] *Id.* at 532–33.

[103] United States v. Cortez, 449 U.S. 411, 417–18 (1981).

[104] *See Montoya de Hernandez*, 473 U.S. at 541–42.

[105] *See* United States v. Cotterman, 709 F.3d 952, 960 (9th Cir. 2013) (en banc) (citing *Montoya de Hernandez*, 473 U.S. at 538).

[106] *See Montoya de Hernandez*, 473 U.S. at 537 (citing New Jersey v. T.L.O., 469 U.S. 325, 337–42 (1985)).

[107] *See Cotterman*, 709 F.3d at 960 (citing United States v. Jacobsen, 466 U.S. 109, 124 (1984)).

[108] *See supra* Section II.B.

[109] *See* Alasaad v. Nielsen, No. 17-CV-11730, 2018 WL 2170323, at *17 (D. Mass. May 9, 2018) (noting that neither the Supreme Court nor the First Circuit have yet held that a warrant is required for any type of border search).

Courts of Appeals that have faced the question have come to contrary conclusions. This Part examines the existing circuit split between the Fourth and Ninth Circuits on one side, and the Eleventh Circuit on the other, over the required level of suspicion necessary for forensic searches of electronics at the U.S. border.

A. Fourth and Ninth Circuits Require Reasonable Suspicion

The first approach to searches of electronic devices at the border is currently shared among the Fourth and Ninth Circuits. Both require reasonable suspicion for forensic searches of electronic devices at the border.

1. Ninth Circuit

In *United States v. Cotterman*, the Ninth Circuit broke ground in requiring reasonable suspicion for forensic searches.[110] Howard Cotterman, a U.S. citizen, presented himself with his wife at a port of entry in Lukeville, Arizona for admission into the United States from Mexico.[111] The Treasury Enforcement Communications System identified Cotterman as a sex offender based on two prior child sex crime convictions from 1992 and flagged him as potentially involved in child sex tourism.[112] During a secondary inspection, border agents retrieved two laptop computers and three digital cameras; the inspection revealed family and other personal photos, in addition to password protected files.[113] In Tucson, an Immigration and Customers Enforcement ("ICE") agent copied the laptops' hard drives and ran software to examine their contents.[114] The agent released the camera, but scrutinized the laptops further.[115] Mr. Cotterman's laptop housed seventy-five images of child pornography within

110 *See Cotterman*, 709 F.3d at 956–57.

111 *See id.* at 957.

112 *See id.* at 956–57.

113 *Id.* at 957–58.

114 *Id.* at 958.

115 *Id.*

unallocated space and 378 images of child pornography contained in twenty-three password-protected files.[116]

After a grand jury indicted Cotterman for offenses related to child pornography, Cotterman moved to suppress the laptop evidence.[117] The district court granted Cotterman's motion.[118] But the Ninth Circuit reversed, finding that the secondary site forensic laptop search did not require reasonable suspicion.[119] In a final twist, the Ninth Circuit sitting en banc endorsed a reasonable suspicion requirement due to the "comprehensive and intrusive nature of a forensic examination," but Cotterman still lost because the court found that the totality of the factors met the requirement.[120] The question for the court, was not so much "where," but "how" the search was conducted.[121] The "how" at issue failed the reasonableness test. The majority referred to the forensic search as a "computer strip search"[122] "akin to reading a diary line by line looking for mention of criminal activity—plus looking at everything the writer may have erased."[123]

While eschewing forensic searches without reasonable suspicion, the court acknowledged the continued practice of suspicionless manual searches approved in *United States v.*

116 *Id.* at 958–59.

117 *Id.* at 959.

118 *Id.*

119 United States v. Cotterman, 637 F.3d 1068, 1083–84 (9th Cir. 2011).

120 *Cotterman*, 709 F.3d at 962, 970. The district court sentenced Cotterman to thirty-five years in prison for child exploitation offenses. *See Man Sentenced to 35 Years in Prison for Child Pornography Offenses*, U.S. DEP'T. OF JUSTICE (Sept. 30, 2014), https://www.justice.gov/usao-az/pr/man-sentenced-35-years-prison-child-pornography-offenses [https://perma.cc/UQ8P-G4NA].

121 Despite its finding of a reasonable suspicion requirement, the Ninth Circuit rejected Cotterman's claim that the second forensic search constituted an unlawful "extended border search" merely because his devices were transported and examined beyond the border, since despite being permitted to depart the border inspection station after the initial search, neither Mr. Cotterman nor his wife cleared customs with their property. *Cotterman*, 709 F.3d at 961. Thus, he did not regain his expectation of privacy as he would have with re-entry. *See id.* at 962.

122 *Id.* at 966.

123 *Id.* at 962–63.

Arnold.[124] In *Arnold*, CBP agents' search of two laptop folders entitled "Kodak Pictures" and "Kodak Memories" was unintrusive because the officers merely had the laptop "booted up" for a quick look inside.[125] As such, while the court advanced the debate over privacy concerns for forensic searches, it left much to be desired from the conversation surrounding privacy intrusions from manual searches.

2. Fourth Circuit

The Fourth Circuit followed in *Cotterman*'s footsteps five years later.[126] In *United States v. Kolsuz*, customs agents detained the defendant, Hamza Kolsuz, at Washington Dulles International Airport after they found firearm parts in his luggage.[127] Kolsuz intended to board a flight to Turkey.[128] Instead, the agents arrested him and subjected his smartphone to a month-long, off-site forensic analysis that yielded a nearly 900-page report.[129] In the United States District Court for the Eastern District of Virginia, Kolsuz was convicted of attempting and conspiring to smuggle firearms out of the country after his motion to suppress the forensic data report was denied.[130]

On appeal, Kolsuz argued that (1) the border exception no longer applied once he and his phone were in government custody, and (2) post-*Riley*, a warrant based on probable cause is required for forensic phone searches.[131] The Fourth Circuit swiftly rejected Kolsuz's first argument, finding that the temporal and spatial distance between Kolsuz and the off-site analysis did not escape the border exception's broad reach.[132]

124 *See* United States v. Arnold, 533 F.3d 1003, 1009 (9th Cir. 2008); *see also Cotterman*, 709 F.3d at 960 (acknowledging approval of "a quick look and unintrusive search of laptops").

125 *Id.* at 1005.

126 *See* United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018).

127 *See id.* at 136.

128 *Id.*

129 *Id.*

130 *Id.*

131 *Id.* at 136–37.

132 *See id.* at 137.

The second argument did not find more success, as the court also found that the post-arrest timing of the search did not trigger *Riley*'s search-incident-to-arrest.[133] The court did find, however, that *Riley* demanded some form of individualized suspicion for forensic searches (whether that form is reasonable suspicion or warrant for probable cause was left unanswered).[134]

The court did pointedly separate "manual" from "forensic." The officers' pre-arrest use of the iPhone's touch screen to scroll through Kolsuz's recent calls and text messages was a manual search.[135] A forensic search, on the other hand, transpired when a computer forensic agent used a Cellebrite Physical Analyzer to extract the following data: "personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz's physical location down to precise GPS coordinates."[136] The court further bolstered this dichotomy by grouping the forensic search with other non-routine searches requiring individualized suspicion, such as "strip searches, alimentary-canal searches, x-rays and the like," and setting them aside from routine searches of luggage and outer clothing.[137] *Kolsuz* may have left the level of individualized suspicion undecided, but this much was made clear: Forensic searches of electronics post *Riley* are non-routine searches meriting heightened special treatment.

133 *See id.* at 142 (citing United States v. Ickes, 393 F.3d 501, 503 (4th Cir. 2005)).

134 *See id.* at 146 ("After *Riley*, we think it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring *some* form of individualized suspicion.") (emphasis added); *see also id.* at 148 ("Accordingly, we need not—and will not—reach the issue of whether more than reasonable suspicion is required for a search of this nature in affirming the judgment of the district court.").

135 *Id.* at 139.

136 *Id.*

137 *Id.* at 144–45.

B. The Eleventh Circuit Requires No Suspicion for Forensic Searches

In an unexpected turn, the Eleventh Circuit unequivocally rejected its sister circuits' approach later that same year, remarking in *United States v. Touset*, "we are unpersuaded."[138] Not only did the Eleventh Circuit find that border agents had reasonable suspicion to search Karl Touset's electronics, but the court squarely rejected any argument that *Riley* required reasonable suspicion.[139] The facts in *Touset* were similar to those in *Cotterman*. In both cases, officers had more than an inchoate and unparticularized suspicion—here, the government knew that Karl Touset sent three low-money transfers to a bank account, that the account in question was associated with a Philippine phone number tied to an email account containing an image of child pornography, and that the Philippines was a popular source country of child pornography.[140] The district court sentenced Touset to ten years imprisonment and lifetime supervision.[141] And as at issue in *Cotterman*, the government subjected Touset's electronics to a forensic search. So why the difference?

The court simply perceived no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement of a like search of personal property, despite obvious qualitative differences. It stated:

> And it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects. The same could be said for a recreational vehicle filled with personal

138 United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018).

139 *Id.* at 1229.

140 *Id.* at 1230.

141 *Id.* at 1231.

> effects or a tractor-trailer loaded with boxes of documents.[142]

The court also rejected the Fourth Circuit's reliance on *Riley* as the fodder for a heightened suspicion requirement.[143] While acknowledging the significant intrusion on one's privacy resulting from a cell phone search, the Eleventh Circuit echoed its recent holding in *United States v. Vergara*, denying *Riley's* applicability to border searches.[144]

Riley aside, the Eleventh Circuit first bluntly categorized a forensic search of an electronic device as a search of property.[145] The court also distinguished property searches from searches of a person's body.[146] In the case of body searches, the Eleventh Circuit examined the "personal indignity" of the search, not its extensiveness.[147] In weighing personal indignity, the court considered several factors, such as physical contact with the agent conducting the search, exposure of intimate body parts, and the use of force.[148] The court then applied these factors to explicitly rebuke *Cotterman's* comparison of a forensic search to a "computer strip search[:]" "[a] forensic search of an electronic device is not like a strip search or an x-ray; it does not require border agents to touch a traveler's body, to expose intimate body parts, or to use any physical force against him."[149]

Lastly, the court made a specific point about child pornography. The court considered a requirement of additional suspicion to be the equivalent of affording "special protection for the property most often used to store and

142 *Id.* at 1233.

143 *See id.* at 1234.

144 *Id.* In *Vergara*, the Eleventh Circuit noted, "the Supreme Court expressly limited its holding [in *Riley*] to the search-incident-to-arrest exception." United States v. Vergara, 884 F.3d 1309, 1312 (11th Cir. 2018).

145 *See* United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) ("Although it may intrude on the privacy of the owner, a forensic search of an electronic device is a search of property.").

146 *See id.* at 1234.

147 *Id.*

148 *See id.*

149 *Id.*

disseminate child pornography."[150] In this case, Touset travelled with multiple laptops, external hard drives, iPhones and a camera.[151] Given the proliferation of child pornography on the internet, law enforcement officers must rely on forensic searches of electronic devices as a common investigatory method[152]—one which the court worried would be impeded by a heightened constitutional requirement of suspicion.[153]

IV. THE SMARTPHONE DIFFERENCE: A SHIFT ON THE SPECTRUM FROM GOVERNMENT INTERESTS TOWARD INDIVIDUAL PRIVACY INTERESTS

As *Riley* makes clear, smartphones are different from other personal belongings.[154] While they fall into a broader classification of electronic devices, they are distinct in their technological makeup and everyday use. The "Swiss army knife" of mobile devices, smartphones are Americans' go-to-devices for a range of activities, from checking social networks to reading the news.[155] Smartphones are held so closely that they have been compared to an additional limb, a "feature of human anatomy."[156] People wake up to their alarms, do not leave their homes without them, and check them on average fifty-two times throughout the day.[157]

The collective information smartphones reveal is astounding: personal conversations via text, private emails,

150 *Id.* at 1235.

151 *Id.* at 1230.

152 *See id.* at 1236.

153 *Id.* (warning that the court "should not invent heightened constitutional protection for travelers who cross our borders with this contraband in tow").

154 *See supra* notes 72–75 and accompanying text.

155 DELOITTE, 2018 GLOBAL MOBILE CONSUMER SURVEY: US EDITION 4 (2018) [hereinafter GLOBAL MOBILE CONSUMER SURVEY], https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-global-mobile-consumer-survey-exec-summary-2018.pdf [https://perma.cc/KR4A-T6VS].

156 Riley v. California, 573 U.S. 373, 385 (2014).

157 GLOBAL MOBILE CONSUMER SURVEY, *supra* note 155, at 3.

financial records and confidential business documents, medical records, web browser history, contacts and call history, location data and history, photos and videos, steps walked, Snaps, and romantic matches.[158] This list goes on. Many of these differences, however, are also applicable to laptops and their tablet cousins, as smartphones are "[e]ssentially tiny computers."[159] Indeed, Cambridge Dictionary defines "smartphone" as "a mobile phone that can be used as a small computer and that connects to the internet[.]"[160] With these factors in mind, courts should reevaluate the border exception as applied to cell phones.

As mentioned in Section II.C, the government's authority to protect the nation from contraband is well-documented. This right, grounded in state-sovereignty, may be "heightened" by "national cris[e]s" ranging from illegal drug-smuggling to international terrorism.[161] While the nexus between the border exception and traditionally excluded contraband like "communicable diseases, narcotics, or explosives"[162] is readily apparent, the line blurs for electronic contraband. Of course, physical contraband may be hidden in the cavities of an electronic device. Such contraband, however, could be revealed during a mandatory conveyor belt security scan. But electronic contraband—an illicit file, for example—is "borderless."[163] At the click of a mouse, it can be sent,

158 *See Smartphone Privacy*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/consumer-guides/smartphone-privacy [https://perma.cc/LY9D-CS6S] (last modified Dec. 19, 2017); *see also* United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) ("They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails").

159 *Smartphone Privacy*, *supra* note 158; *see also Riley*, 573 U.S. at 393 (characterizing cell phones as "minicomputers that also happen to have the capacity to be used as a telephone").

160 *Smartphone*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/smartphone [https://perma.cc/Z2FG-YHQH].

161 *Cotterman*, 709 F.3d at 966 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985)).

162 *Montoya de Hernandez*, 473 U.S. at 544.

163 United States v. Vergara, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, Jill, J., dissenting).

opened, and viewed without ever physically crossing the United States border.[164]

The border search exception for property is not as absolute as the Eleventh Circuit maintains.[165] Eventually, a "search initiated at the border could become so attenuated from the rationale for the border search exception that it no longer would fall under the exception."[166] With the exception of child pornography—which is "borderless"—most searches of smartphones merely *further* the potential for discovery of physical contraband.[167] While the order of discovery in *Kolsuz* is in reverse (the agents found firearm parts first, then conducted an electronics search),[168] the distinction between physical contraband and evidence thereof is nonetheless apt. If the search does not reveal contraband itself, but rather the location of contraband inside the border, it is one degree removed from the border search's aim to "protect[] this Nation from entrants who may bring *anything* harmful into this country[.]"[169] The more attenuated the rule is from its underlying justification of territorial integrity, the greater the shift toward individual privacy interests should be. The national security interests of keeping out "borderless" electronic contraband are arguably lesser than those of keeping out bombs or tuberculosis due to the nature of the particular dangers posed by "readily transportable chemical and biological weapons."[170] Similarly, the privacy interests inherent in a smartphone's vast ecosystem of personal

164 *See id.*

165 *See supra* notes 142–44 and accompanying text.

166 United States v. Kolsuz, 890 F.3d 133, 143 (4th Cir. 2018) (citing United States v. Molina-Isidoro, 884 F.3d 287, 295–97 (5th Cir. 2018) (Costa, J., concurring)).

167 *See* CBP DIRECTIVE, *supra* note 4, § 1 (recognizing that some searches may further the retrieval of evidence helpful in combating terrorist activity).

168 *See Kolsuz*, 890 F.3d at 136.

169 *Montoya de Hernandez*, 473 U.S. at 544 (emphasis added).

170 United States v. Alfaro-Moncada, 607 F.3d 720, 730 (11th Cir. 2010).

information are likely greater than those present in a carry-on duffle bag.

V. REASONABLE SUSPICION FOR MANUAL AND FORENSIC SEARCHES OF NON-FULLY CURATED DEVICES ("NFCDS")

Part V now takes the smartphone difference to its natural conclusion: Suspicionless searches of smartphones and laptops at the border no longer make sense. Smartphones and like devices, therefore, should be set apart from other possessions that fit comfortably within the border search exception regime. Section V.A argues that reasonable suspicion for both manual[171] and forensic searches of smartphones and related devices is the appropriate standard that courts should employ. Section V.B distinguishes smartphones and their sister electronics from other electronics, both in their storage capacity and curability. Section V.C, however, posits that probable cause is too extreme a standard given the practical realities of the United States border. Finally, Section V.D explains why electronic devices that are fully curable—such as cameras—do not merit the same heightened suspicion and should be treated like any ordinary luggage piece subject to suspicionless searches at the border.

A. The Current Distinction Between Manual and Forensic Searches of Cell Phones and Laptops Is Inapposite

The privacy concerns articulated in *Riley*—access to an individual's health-related browsing or location history[172]—are not limited to forensic searches. A forensic search is more intrusive than a manual search, as it may unearth deleted files and analyze large quantities of data. But a sensitive work

171 *See supra* notes 4–5 and accompanying text (discussing manual searches).

172 *See* Riley v. California, 573 U.S. 373, 396–97 (2014).

email, or the "significant locations" on your iPhone can be accessed without such a search.[173]

The Ninth Circuit's distinction between manual and forensic searches, therefore, does not hold water. The *procedure* of these two types of searches is, indeed, easily distinguishable. Officers may use common sense when differentiating between a manual review of files by hand and application of computer software to analyze the device.[174] But the rationale behind the suspicion jump "is left unexplained."[175] Simply perusing an average smartphone user's mobile application software ("apps") by hand could easily reveal the "wealth of detail about her familial, political, professional, religious, and sexual associations" that the Supreme Court has considered worthy of Fourth Amendment protection.[176]

Courts differentiating between manual searches and exhaustive forensic searches cite the "cursory" or "quick look" nature of manual searches.[177] They fail to mention, however, that although the search in *Cotterman*, for example, was short in time relative to the longer forensic search, not *all* manual searches are, in fact, "cursory." Further, even a fast scan can reveal precisely the type of sensitive information *Riley* deems special. For example, two of the plaintiffs in *Alasaad v. Nielsen*, a civil case currently pending before the United States District Court for the District of Massachusetts, allege manual searches lasting about two hours, while a third

173 "Significant Locations" permits "[y]our iPhone [to] keep track of places you have recently been, as well as how often and when you visited them, in order to learn places that are significant to you." Location Services & Privacy, APPLE (Mar. 25, 2019), https://support.apple.com/en-us/HT207056 [https://perma.cc/2GYM-NVNL]. While they cannot be read by Apple, "Significant Locations" would be easily viewable by a customs agent with access to the phone. *See id.*

174 *See* United States v. Cotterman, 709 F.3d 952, 967 (9th Cir. 2013).

175 *Id.* at 981 (Smith, J., dissenting).

176 *See* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

177 *See Cotterman*, 709 F.3d at 960; United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 502 (4th Cir. 2005).

plaintiff reports officers seizing his phone for about *four* hours.[178] Moreover, yet another plaintiff allegedly withstood a manual search for one-and-one-half hours, but it would only have taken agents mere seconds to open her smartphone photo album and access private photographs of her without her headscarf.[179] If the heart of the concern as articulated in *Riley* is the "cache of sensitive personal information"[180] on a smartphone, then *Cotterman's* forensic search requirement should be rethought.

Some are beginning to challenge the black and white divide between manual and forensic searches.[181] Although bound by *Cotterman*'s holding, the district court in *United States v. Caballero* lamented that if it "were free to decide the question in the first instance, it would hold that the warrantless [manual] cell phone search under these circumstances would be unreasonable."[182] Another district court, in *United States v. Ramos*, suggested that applying *Cotterman's* reasonable suspicion standard to all border searches of cell phones "may be a prudent way to harmonize *Riley*'s concerns with the salutary border search principles."[183]

178 *See* Alasaad v. Nielsen, No. 17-CV-11730, 2018 WL 2170323, at *6–7 (D. Mass. May 9, 2018).

179 *See id.* at *5.

180 Riley v. California, 573 U.S. 373, 395 (2014).

181 *See* Eunice Park, *The Elephant in the Room: What Is A "Nonroutine" Border Search, Anyway? Digital Device Searches Post-*Riley, 44 HASTINGS CONST. L.Q. 277, 312–14 (2017); *see also* United States v. Caballero, 178 F. Supp. 3d 1008, 1017 (S.D. Cal. 2016).

182 *Caballero*, 178 F. Supp. 3d at 1017. The circumstances involved a post-arrest manual search of defendant's cell phone which revealed a photograph of a large sum of money. *Id.* at 1011–12.

183 United States v. Ramos, 190 F. Supp. 3d 992, 1002 (S.D. Cal. 2016).

B. The Luggage Piece: Why Smartphones and Like Devices Deserve More Protection Than Other Electronic Devices

1. Storage Capacity

Quantity matters. While a "recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents"[184] indeed contain a very large number of items, the scale is dwarfed by the amount of information on smartphones and laptop hard drives.[185] Smartphones have internal memory capacities of up to 128 gigabytes,[186] while laptop drives can range from 160 gigabytes to over two terabytes in capacity.[187] To put this quantity in perspective, one gigabyte is equivalent to a single pick-up truck full of paper, whereas one terabyte (1000 gigabytes) is the volume of paper produced from a forest of 50,000 trees.[188] In other words, one hard drive may hold the paper equivalent of more than twice the number of trees in Central Park.[189] The absolute difference between one tractor-trailer and one hundred matters less than how that increased quantity

184 United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).

185 *See* United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) ("The average 400–gigabyte laptop hard drive can store over 200 million pages . . . . [and] [e]ven a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, ever-increasing, capacity of digital storage").

186 Davidson v. Apple, Inc., No. 16-CV-04942, 2018 WL 2325426, at *21 (N.D. Cal. May 8, 2018).

187 Mark Kyrnin, *Guide to Laptop Storage Drives*, LIFEWIRE (Nov. 15, 2018), https://www.lifewire.com/laptop-storage-drives-guide-833445 [https://perma.cc/Q7WP-35V7].

188 Tony R. DeMars, *Big Data*, *in* COMMUNICATION TECHNOLOGY UPDATE & FUNDAMENTALS 305, 307 (August E. Grant & Jennifer H. Meadows eds., 2018).

189 *See* Jessica Sain-Baird, *What Are Central Park's Most Colorful Fall Trees?*, CENTRAL PARK CONSERVANCY BLOG (Oct. 4, 2018), http://www.centralparknyc.org/about/blog/most-colorful-trees.html [https://perma.cc/AR7M-9YSD].

changes the practicality of deleting or temporarily moving files.[190]

2. Curability

To more precisely distinguish between traditional luggage and electronic devices, this Note proposes separating devices into two broad categories: (1) Non-Fully Curated Devices ("NFCDs"), such as smartphones, laptops, tablets, and wearables, and (2) Fully Curated Devices ("FCDs"), such as digital and video cameras, GoPros, eReaders, thumb-drives and floppy disks, and portable game consoles. "Curate" is defined as "select[ing] things such as documents, music, products, or internet content to be included as part of a list or collection."[191] Indeed, it is the point of curating, or actively choosing, that most strongly separates NFCDs from traditional luggage and therefore justifies a special treatment of reasonable suspicion for manual and forensic searches. When one travels, one decides "what papers to take and what to leave behind."[192] This is easily done when packing a suitcase or briefcase, but is far more difficult with a smartphone or laptop. It is true that a user may delete or transfer certain files in anticipation of travel, making the device partially-curated. But, not only may the task of removing unnecessary files prove to be an impractical solution given the volume, it may actually be unfeasible given the two-way nature of information sharing facilitated on many NFCDs.[193] Users do not stop receiving emails, photographs, Snapchats, texts, calls, dating app matches, or payment

190 United States v. Cotterman, 709 F.3d 952, 987 (9th Cir. 2013) (Smith, J., dissenting) (citing United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008) ("[C]ase law does not support a finding that a search which occurs in an otherwise ordinary manner, is 'particularly offensive' simply due to the storage capacity of the object being searched.").

191 *Curate*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/curate [https://perma.cc/MC7T-9FEY].

192 *Cotterman*, 709 F.3d at 965.

193 *See generally* Editorial, *Smartphones and the 4th Amendment*, N.Y. TIMES (Apr. 27, 2014), https://www.nytimes.com/2014/04/28/opinion/smartphones-and-the-4th-amendment.html [https://perma.cc/Y8FS-RZAT].

requests from friends at the airport *after* they decide what to bring and what to leave. Smartphones are analogous to a world in which family, business associates, and friends could continuously add items to a traveler's suitcase from anywhere without the traveler's knowledge. A person's "expectation of privacy is less at the border,"[194] but it is not null; the inconvenience of standard screening procedures pales in comparison to a peek inside a traveler's communications and electronic papers—which they may have not even yet viewed.

In addition to the potential for the receipt of new files, an individual's smartphone itself may amass data unbeknownst to its users.[195] Smartphones are packed with sensors that automatically read the phone's surroundings such as light, pressure, temperature, and proximity to other objects.[196] This data may seem non-threatening, but it is vulnerable to abuse: Google Play recently banned twenty apps from Android phones that could "record with the microphone, monitor a phone's location, take photos, and then extract the data,"[197] all without the user's knowledge. Sensor data collection not only raises concerns of outside spying, but further spotlights users' loosening grip over their non-curated data.

The curation argument is analogous to the voluntary sharing argument raised in *Carpenter*.[198] Just as it is unreasonable to expect that a cell phone user "voluntarily" shares her "comprehensive dossier of physical movements" merely by powering on the smartphone,[199] it is unreasonable to equate the affirmative act of packing a suitcase to preparing a smartphone for travel. Moreover, despite the sky-high number of smartphone owners, knowledge of how the devices

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

195 Maria Temming, *Your Phone Is Like a Spy in Your Pocket*, SCIENCE NEWS (Jan. 23, 2018), https://www.sciencenews.org/article/smartphones-data-collection-security-privacy [https://perma.cc/SK8P-G9L3].

196 *Id.*

197 *Id.*

198 *See supra* note 89 and accompanying text.

199 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

work varies.[200] If it is virtually impossible for a traveler to be fully aware of her NFCD's universe of data, neither she nor those with lesser technological literacy can be fully aware.

C. A Warrant Requirement, However, Is Impractical at the Border

There is not a single case suggesting that a border search—no matter how invasive—requires *more* than reasonable suspicion.[201] Indeed, the highest standard that the Supreme Court has applied at the border is reasonable suspicion.[202] Nearly five years have passed since *Riley*, and while courts have disagreed over whether forensic searches merit increased suspicion, they all appear to stop shy of probable cause or choose to avoid the question.[203] That is not to say, however, that Congress cannot decide otherwise. Two proposed bills advocate for probable cause warrants with respect to forensic searches.[204]

Nonetheless, warrants face greater practicability concerns at the border. Obtaining warrants at the border is more burdensome due to the large volume of items moving across the border with the added difficulty of obtaining a warrant when the subject of the search is mobile.[205] Furthermore, the

200 *See* Paul E. Ketelaar & Mark van Balen, *The Smartphone as Your Follower: The Role of Smartphone Literacy in the Relation Between Privacy Concerns, Attitude and Behaviour Towards Phone-Embedded Tracking*, 78 COMPUTERS IN HUM. BEHAV. 174, 175 (2018).

201 *See* United States v. Molina-Isidoro, 884 F.3d 287, 292 (5th Cir. 2018) ("[N]o post-*Riley* decision . . . has required a warrant for a border search of an electronic device.").

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

203 *See supra* Section III.A.2.

204 *See* Protecting Data at the Border Act, S. 823, 115th Cong. (2017) (arguing for a warrant for manual and forensic searches); S. 2462, 115th Cong. (2018) (arguing for reasonable suspicion prior to basic or manual searches and a probable cause warrant for forensic searches).

205 *See* Carroll v. United States, 267 U.S. 132, 153 (1925) (allowing the search of a vehicle without a warrant when obtaining one before the vehicle left the area was impracticable).

exigent circumstances doctrine,[206] which excuses compliance with the Fourth Amendment's warrant requirement, overlaps with the border exception. Many national security interests propping up the border exception also create exigent situations and therefore could separately caution against a warrant requirement.[207] Moreover, while the process of obtaining warrants is becoming increasingly speedy with the use of electronic warrant applications, such alternatives are not available in every state.[208]

D. No Suspicion for FCDs

Cameras, iPods, thumb-drives, GoPros, e-readers, and handheld game consoles are all fully curated devices in the sense that users have the capacity of knowing—and curating—the devices' contents. In *Cotterman*, the officer could open and view image files on *Cotterman's* cameras while the Cottermans waited to enter the country.[209] Little would have changed if Cotterman brought these photographs in traditional print photo albums. If an international traveler can mitigate the intrusion occasioned by a routine luggage search by leaving behind certain photographs or other contraband, she can also choose which photos to keep on her camera.

Indeed, Judge Amy Coney Barrett alluded to this critical distinction during oral arguments in a Seventh Circuit child

206 *See* Mincey v. Arizona, 437 U.S. 385, 393–94 ("[W]arrants are generally required to search a person's home or his person unless 'the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment.").

207 *See* Laura Nowell, Note, *Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border*, 71 FED. COMM. L.J. 85, 101 (2018) ("The knowledge of an imminent threat to public safety creates the circumstances necessary to invoke the exigent circumstances and justifies a search without a warrant[.])"

208 *See* Missouri v. McNeely, 569 U.S. 141, 172 (2013) (noting that "[a]t least 30 States provide for electronic warrant applications").

209 *See* United States v. Cotterman, 709 F.3d 952, 957–58 (9th Cir. 2013).

pornography case, *United States v. Wanjiku,* when she questioned defense counsel about whether a digital camera lacked *Riley* concerns, such as sensitive browsing history.[210] Unlike a smartphone, a camera is not vulnerable to the unknowing receipt of another's photographs.[211] Moreover, a camera does not map historical travel patterns, group photos by location, or pin them to a digital map.[212]

Requiring no suspicion for searches of FCDs has practical implications for the way Americans travel and make pre-departure decisions. In choosing whether to travel with personal photos, any added benefit from printing and carrying the photographs or storing them on a camera must be counterbalanced with the cost of a heightened search risk. The

[210] Oral Argument at 6:25, United States v. Wanjiku, 919 F.3d 472 (7th Cir. 2019), https://www.courtlistener.com/audio/59635/united-states-v-donald-wanjiku/ [https://perma.cc/Q9PW-48U4]. In *Wanjiku*, the Seventh Circuit refused to adopt either Wanjiku's position that a forensic search of his electronics required probable cause or the government's position that such searches require no suspicion at all; instead, the court upheld the lower court's denial of Wanjiku's motion to suppress evidence from his electronics because the agents acted in good faith when they conducted the search with reasonable suspicion at a time when no court had ever required more. *See Wanjiku*, 919 F.3d 472.

[211] For example, WhatsApp is a cross-platform instant messaging app that relies on the internet. In January 2017, the app had more than 1.2 billion monthly active users worldwide. *WhatsApp – Statistics & Facts*, STATISTA, https://www.statista.com/topics/2018/whatsapp/ [https://perma.cc/X6ZY-VMJL]. Photographs and videos sent over WhatsApp appear immediately in the recipient's photo gallery. *See Configuring Auto Download,* WHATSAPP, https://faq.whatsapp.com/en/android/23248698/?category=5245251 [https://perma.cc/Q4HF-D7KG]. "By default, WhatsApp will automatically download images over your cellular connection to provide you with quick access to your latest photos." *Id.* "Automatically downloaded media will show up in your gallery." *Id.*

[212] "The iOS Photos app automatically groups pictures you take into a Places album – as long as you have the location services feature enabled on your phone when you are snapping your shots. The Photos software reads the GPS information embedded in each picture file to sort images, and then displays the images accordingly on a map within the app." J.D. Biersdorfer, *Put Your iPhone Photos on the Map*, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/personaltech/put-your-iphone-photos-on-the-map.html [https://perma.cc/V6E4-U6VS].

calculus is necessarily more complicated when travel isn't strictly for leisure. To the extent that businesses entrust their employees with sensitive business information, such information would be more vulnerable to unintended review by officers if housed, for example, on a company USB flash drive than on a laptop. Thumb drives may garner less attention alongside the growth of NFCDs, but the global flash memory market is projected to see growth over the next few years, so they should not be discounted in the near term.[213]

Critics may point out that it may be difficult to distinguish between NFCDs and FCDs, with some sub-categories of electronic devices falling into a gray area.[214] However, TSA agents are trained to distinguish between many prohibited and allowed property items, and travelers likewise must pay careful attention to fluid ounce requirements and security line instructions.[215] Therefore, it is not unreasonable for a traveler to understand that her camera and smartphone might be subject to different suspicion thresholds under the Fourth Amendment.

Despite advances in NFCDs, such as the smartphone's photography capability, the camera market is expected to

[213] In 2021, the flash memory market is expected to be worth $64.24 billion U.S. dollars worldwide. *See Flash Memory Market Revenues Worldwide from 2013 to 2021 (in Billion U.S. Dollars)*, STATISTA, https://www.statista.com/statistics/553556/worldwide-flash-memory-market-size/ [https://perma.cc/7GZB-79KA].

[214] One could argue, for example, that certain Kindles are not e-readers, but tablets. Indeed, this is true of a Kindle Fire. But this distinction is not too difficult to make. While e-readers are designed for reading e-books, tablets offer a whole suite of features, in addition to reading e-books, such as e-mail and web access. *See generally* Marc Saltzman, *E-Book Readers vs Tablets: Which One Is Right for You?*, USA TODAY (Feb. 23, 2014), https://www.usatoday.com/story/tech/columnist/saltzman/2014/02/23/ereaders-vs-tablets/5575963/ [https://perma.cc/7QS9-XLGE].

[215] The TSA Academy trains its employees through props, including prohibited and non-prohibited travel items under various mock scenarios. *See* Rachel Gillett, *'You're at War': I Went Inside the New TSA Academy, Where Officers Learn to Detect Bombs, Spot Weapons, and Find Out Why Failure Isn't an Option*, BUS. INSIDER (Aug. 25, 2016), https://www.businessinsider.com/tsa-academy-airport-security-training-2016-8 [https://perma.cc/2GWG-YCCM].

continue growing over the next four years. Indeed, the high-speed camera market, valued at $288 million in 2018, is projected to reach $422 million by 2023.[216] Therefore, the curability standard may not be the solution ten years from now. But given the healthy market growth forecast for at least certain FCDs, they are likely to continue to accompany travelers internationally and remain vulnerable to illegal misuse.

VI. CONCLUSION

The current circuit split over the degree of suspicion required for forensic searches of electronic devices is deeply problematic. It is grossly unjust that a traveler arriving in Miami maintains a diminished expectation of privacy in their electronics compared to a traveler arriving in San Francisco. In light of the Supreme Court's decisions in *Riley* and *Carpenter*, the unique privacy concerns presented by smartphones and related devices belie the common sense of a suspicion gap between manual and forensic searches. But the solution cannot stop at a reasonable suspicion requirement for *all* searches of electronic devices as a categorical matter. Because FCDs (such as digital cameras) do not pose the same privacy risks as NFCDs (such as smartphones), it is reasonable for a traveler to expect a suspicionless search of the files with which she elects to travel.

The CBP directive could help fix this gap in the case law, and is subject to review and potential modifications every three years.[217] The current directive defines "electronic device" as "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication

---

[216] *High-speed Camera Market by Usage, Frame Rate (1,000–5,000, >5,000–20,000, >20,000–100,000, >100,00), Resolution (2-5MP, and >5MP), Throughput, Component, Accessory, Application, and Geography – Global Forecast to 2023*, RES. & MKTS., (Nov. 2018), https://www.researchandmarkets.com/research/g9n6br/highspeed_camera?w=4 [https://perma.cc/9BZA-JVWG].

[217] *See* CBP DIRECTIVE, *supra* note 4.

devices, cameras, music and other media players."[218] In light of the differences between NFCDs and FCDs and the Supreme Court's special recognition of modern cell phones in *Riley* and *Carpenter*, drafters should consider revising this language to account for the privacy concerns specific to NFCDs.

[218] *Id.* § 3.2.