The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study

Matthew B. Kugler†

It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity.

United States v Flores-Montano[1]

It is frightening the number of ways I had not even considered being "violated" prior to this survey.

Subject 189[2]

INTRODUCTION

The Fourth Amendment protects the right of individuals to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[3] The recurring question in Fourth Amendment jurisprudence, then, is the reasonableness of a given search in a given context. This Comment analyzes the reasonableness of searches of electronic devices—smartphones, laptops, and tablets—in the context of a border crossing. When a traveler enters the country, whether at an airport or a land border, how much protection should the contents of his or her electronic gadgets be given? Historically, all of a traveler's possessions could be thoroughly searched, even without cause, because Fourth Amendment protections are substantially relaxed at the border.[4] But, given the sheer amount of personal information that can be recovered from a smartphone's text message log or a computer's e-mail archive, is it "reasonable" to give government

† BA 2005, Williams College; PhD 2010, Princeton University; JD Candidate 2015, The University of Chicago Law School.

1 541 US 149, 153 (2004).

2 A participant in the empirical study that forms the basis of this Comment, after rating the intrusiveness of various border searches. See note 198.

3 US Const Amend IV.

4 See *United States v Montoya de Hernandez*, 473 US 531, 538–40 (1985).

agents unfettered discretion to search the contents of electronic devices?

A recent court opinion proposed that such searches should require an elevated level of suspicion; border agents would not be able to conduct the search unless they had some specific reason to suspect the traveler of wrongdoing.[5] Scholars advocating for this type of elevated-suspicion standard base their arguments on the role that electronic devices now play in daily life, the degree of intrusion into the privacy and dignity of the individuals being searched, and the potential for surprise.[6] Courts have recognized the importance of these factors in evaluating the reasonableness of border searches, particularly the degree of intrusion on privacy and dignity interests.[7] When applying these criteria to searches of electronic devices, however, courts have disagreed on the magnitude of the privacy intrusion. In *United States v Cotterman*,[8] for instance, the Ninth Circuit said that "[i]nternational travelers certainly expect that their property will be searched at the border. What they do not expect is that, absent some particularized suspicion, agents will mine every last piece of data on their devices or deprive them of their most personal property for days."[9] Based on this assessment, the Ninth Circuit then concluded that some searches of electronic devices represent a "substantial intrusion" on privacy and dignity and should therefore require elevated suspicion.[10] Other courts, however, have disputed the notion that travelers find searches of electronic devices any more intrusive or surprising than searches of their other possessions and have therefore not reached the same result.[11]

This Comment presents the results of an empirical study of approximately three hundred adult Americans that measures the perceived intrusiveness of electronic-device searches and the

---

5 See *United States v Cotterman*, 709 F3d 952, 960 (9th Cir 2013) (discussing the appropriate level of suspicion for searching electronic devices at the border).

6 See, for example, John W. Nelson, *Border Confidential: Why Searches of Laptop Computers at the Border Should Require Reasonable Suspicion*, 31 Am J Trial Advoc 137, 141–42 (2007) (discussing laptops as an extension of the person); Rasha Alzahabi, Note, *Should You Leave Your Laptop at Home When Traveling Abroad? The Fourth Amendment and Border Searches of Laptop Computers*, 41 Ind L Rev 161, 179–81 (2008) (discussing the unprecedented breadth of private information stored on laptops).

7 See, for example, *United States v Flores-Montano*, 541 US 149, 152 (2004).

8 709 F3d 952 (9th Cir 2013).

9 Id at 967.

10 Id at 968.

11 See, for example, *United States v Ickes*, 393 F3d 501, 502–06 (4th Cir 2005).

actual expectations of ordinary citizens. The results show that people see the intrusiveness of electronic-device searches as comparable to that of strip searches and body cavity searches, which have generally been held to require elevated suspicion.[12] Electronic searches are the *most* revealing of sensitive information and are only slightly less embarrassing than the most intimate searches of the body.[13] These searches, therefore, implicate the types of privacy and dignity concerns that the Supreme Court has stated may lead to an elevated-suspicion requirement.[14] Also, most people believe that their electronic devices are not subject to search without cause at a border crossing.[15] Just as the Ninth Circuit feared in *Cotterman*,[16] the study suggests a substantial chance of unfair surprise. By presenting the actual views and expectations of Americans, these data help quantify the civil liberty concern that is being weighed against the government's interest in securing the border.

These data are also relevant to a closely related issue in Fourth Amendment law. The Supreme Court recently ruled on searches of cell phones incident to arrest in *Riley v California*.[17] There, as in the border search context, the central claim of privacy proponents was that electronic devices are different than the address books, grocery lists, and briefcases that prior doctrines were designed to handle.[18] That claim was endorsed in Chief Justice John Roberts' majority opinion, which held that cellular phones could not be searched incident to arrest without a warrant or exigent circumstances.[19] Though many issues relevant to searches incident to arrest are beyond the scope of this Comment, the data discussed here do support a key point: searches of sophisticated electronic devices are almost unique in their intrusiveness.

Part I reviews the contours of the border search exception, examining the types of cases that gave rise to the exception. Part II examines the efforts of courts to apply existing doctrine

---

12 See notes 51–54 and accompanying text.

13 See Table 1.

14 See text accompanying notes 68–85.

15 See pp 1195–96.

16 See *Cotterman*, 709 F3d at 967.

17 No 13-132, slip op (US June 25, 2014).

18 See Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L Rev 27, 36–44 (2008); Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 Santa Clara L Rev 183, 214–22 (2010).

19 *Riley*, No 13-132, slip op at 8–10.

to the novel issues presented by searches of electronic devices. Part III presents the results of the abovementioned empirical survey, measuring actual expectations, attitudes, and beliefs regarding searches of electronic devices at the border. Part IV considers the implications of these results for the border search doctrine.

I. THE BORDER SEARCH EXCEPTION

Though the issues involved in searches of electronic devices are new, the border search exception itself has a rich doctrinal history. To begin, this Part will review the general case law on border searches. It will then show how it has been applied to searches of electronic devices.

"A search or seizure is ordinarily unreasonable" absent "individualized suspicion of wrongdoing;" the police cannot simply enter and search your house.[20] There are a number of important exceptions to this general rule, however, and in practice many searches are conducted without a warrant or probable cause.[21] Border searches have historically been viewed as one exception to the individualized-suspicion requirement. Routine border searches can occur absent any individualized suspicion because "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[22] Nonroutine, more invasive searches may require a showing of a low level of individualized suspicion called "reasonable suspicion."[23]

A. History of the Exception

The exception to the individualized-suspicion requirement for border searches traces its origin to an act of the First Congress. This law established a series of customs offices and gave officials "full power and authority" to enter and search "any ship or vessel, in which they shall have reason to suspect any goods, wares, or merchandise subject to duty shall be concealed" and to secure any such items that were found.[24] The act specifically

---

[20] *City of Indianapolis v Edmond*, 531 US 32, 37 (2000).

[21] Exceptions relevant here include investigative stops, *Terry v Ohio*, 392 US 1, 27 (1968), and searches incident to arrest, *New York v Belton*, 453 US 454, 460 (1981) (permitting searches of automobile passenger compartments incident to arrest). But see generally *Arizona v Gant*, 556 US 332 (2009) (limiting, and possibly abrogating, *Belton*).

[22] *United States v Flores-Montano*, 541 US 149, 152 (2004).

[23] *United States v Montoya de Hernandez*, 473 US 531, 541 (1985).

[24] Act of July 31, 1789 § 24, 1 Stat 29, 43, repealed by Act of Aug 4, 1790 § 74, 1 Stat 145, 178.

differentiated between searches conducted on ships at ports of entry—where "full power and authority" were directly granted without need for judicial oversight—and those of "any particular dwelling-house, store, building, or other place" for which the agents needed to obtain a warrant.[25] Therefore, searches at the border could be conducted at the discretion of the customs agents, whereas searches by customs agents for smuggled goods at nonborder locations were subject to an external warrant requirement. This waiver of the warrant requirement at the border is the core of the border search exception, and it has been in place since 1789. The Supreme Court has repeatedly pointed to the long history of the border search exception as support for its constitutionality.[26]

The main wave of modern border search cases has concerned the smuggling of controlled substances. In the Prohibition-era case *Carroll v United States*,[27] the Court used the border search doctrine as a point of comparison in devising a new exception to the warrant requirement for the search of automobiles.[28] The *Carroll* Court said that "[t]ravelers may be so stopped [without cause] 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."[29] Automobile searches, in contrast, were held to require probable cause (though not a warrant) because the state does not have the same set of strong interests in the nation's interior that it does at the border, where a search is presumptively reasonable even without probable cause.[30]

The Court echoed *Carroll* over fifty years later in *United States v Ramsey*,[31] stating that the sovereign has a strong interest

---

25 Act of July 31, 1789 § 24, 1 Stat at 43.

26 See, for example, *United States v Ramsey*, 431 US 606, 616–17 (1977) (noting that the First Congress also proposed the Bill of Rights, and that the First Congress therefore can be presumed not to have thought the act inconsistent with the Fourth Amendment); *Boyd v United States*, 116 US 616, 623 (1886) (observing that "the seizure of goods forfeited for a breach of the revenue laws . . . has been authorized by English statutes for at least two centuries past").

27 267 US 132 (1925).

28 See id at 153–54. The case concerned the smuggling of alcohol during Prohibition. See id at 159–60.

29 Id at 154.

30 See id.

31 431 US 606 (1977).

in controlling "who and what may enter the country."[32] The case concerned the discovery of illegal drugs in a package mailed to the United States from Thailand.[33] By statute, postal inspectors had the power to open packages and inspect their contents without a warrant if they had "reasonable cause to suspect" that the package contained contraband.[34] In holding the statute constitutional, the Court stated that the proposition "[t]hat searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration."[35]

The defendant in *Ramsey* attempted to raise a First Amendment challenge to the mail inspection because his "papers" (the mail) were subject to search without a warrant, which could potentially have chilling effects on protected expression.[36] The governing statute in the case barred postal inspectors from reading any letters that were inside the packages that they inspected, however;[37] the "papers" contained in the mail were accorded greater protection than the goods and would not be read without a warrant. Because reading the mail was prohibited by the statute and had not occurred in Ramsey's case, the Court explicitly did not reach the First Amendment issue.[38] This question—whether certain types of border searches implicate core civil liberty concerns and should therefore be restricted—underlies many of the more recent border search cases.

B. Requirement of Reasonable Suspicion for Nonroutine Searches

As suggested by the limitation described in *Ramsey* on reading correspondence found in searched packages, not all border searches are alike. Some searches—those considered nonroutine—are permissible only if the border agent has reasonable suspicion.

---

32 Id at 620.

33 Id at 609.

34 Id at 611, quoting 19 USC § 482.

35 *Ramsey*, 431 US at 616.

36 See id at 623–24.

37 See id at 623.

38 See id at 624.

The term "reasonable suspicion" has its origin in the *Terry v Ohio*[39] investigative stop case.[40] It is defined as "a particularized and objective basis for suspecting the particular person stopped of criminal activity."[41] Though a lesser standard than probable cause, it requires the officer to be able to articulate something more than an "inchoate and unparticularized suspicion, or 'hunch.'"[42] Reasonable suspicion generally cannot be based purely on demographic characteristics, but it can be found if the suspect fits a detailed offender profile.[43]

Two Supreme Court cases help define the category of nonroutine searches—those that are so intrusive that they cannot be conducted without reasonable suspicion of wrongdoing. In *United States v Montoya de Hernandez*,[44] the Court considered the case of an alimentary canal smuggler. The defendant, Montoya de Hernandez, entered the United States at Los Angeles International Airport, having come from Bogota, Colombia.[45] Upon arrival, she aroused suspicion based on inconsistencies and implausibilities in her story.[46] Based on his past experience, the customs inspector came to believe that Montoya de Hernandez was likely to be smuggling balloons full of drugs in her digestive tract.[47] She was offered the choice of leaving the country, submitting to an x-ray, or producing a monitored bowel movement.[48] Logistical problems ultimately prevented her from being able to take the first option, and she was detained for approximately sixteen hours before the customs officials sought a warrant for an x-ray.[49] Though the warrant was granted eight hours later, the defendant involuntarily produced a bowel movement that contained the first of many cocaine-filled balloons before the x-ray could take place.[50]

---

39 392 US 1, 37 (1968).

40 Id.

41 *United States v Cortez*, 449 US 411, 417–18 (1981).

42 *Terry*, 392 US at 27.

43 See *United States v Sokolow*, 490 US 1, 10 (1989).

44 473 US 531 (1985).

45 Id at 532.

46 See id at 533 (observing, for instance, that the respondent claimed that she was traveling to the United States to purchase goods for her husband's store but had no appointments scheduled with vendors or suppliers).

47 Id at 534.

48 *Montoya de Hernandez*, 473 US at 534–35.

49 Id at 535.

50 Id at 534–36.

The question before the Court was whether the detention (which at minimum had to be measured as sixteen hours) was justified. The Court held that it was, but only because the customs official could "reasonably suspect" that the traveler was smuggling contraband in her alimentary canal.[51] Because a warrant was obtained before a medical examination was ordered,[52] the Court specifically did not consider what level of scrutiny, if any, would be needed for a body cavity or strip search.[53] Given that reasonable suspicion was required for the detention, however, it is improbable that a lower standard would be appropriate. Courts considering the question after *Montoya de Hernandez* have held that reasonable suspicion is required for strip searches and body cavity searches at the border.[54]

The general rule from *Montoya de Hernandez* is that the reasonableness of a search is determined by balancing the intrusion on the individual's Fourth Amendment interests against governmental interests.[55] What is reasonable under the Fourth Amendment generally "depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself."[56] At the border, however, the test is "qualitatively different" in that the balancing of interests is struck "much more favorably to the Government."[57] This is why routine border searches are not subject to any requirement of reasonable suspicion or probable cause.[58] In the Court's words, the border search cases "reflect longstanding concern for the protection of the integrity of the border."[59] And, in this case, the concern was heightened by the "national crisis" caused by the smuggling of illegal narcotics.[60] For these reasons, the detention was permissible given that reasonable suspicion was present.

---

51 Id at 541.

52 *Montoya de Hernandez*, 473 US at 534–36.

53 See id at 541 & n 4.

54 See, for example, *Tabbaa v Chertoff*, 509 F3d 89, 98 (2d Cir 2007) (observing that strip and body cavity searches generally require reasonable suspicion); *United States v Ramos-Saenz*, 36 F3d 59, 61 (9th Cir 1994) (concluding that strip searches at the border go "beyond the routine"); *United States v Johnson*, 991 F2d 1287, 1292 (7th Cir 1993) (noting that strip and body cavity searches are intrusive and "nonroutine").

55 See *Montoya de Hernandez*, 473 US at 537.

56 Id, citing *New Jersey v T.L.O.*, 469 US 325, 337–42 (1985).

57 *Montoya de Hernandez*, 473 US at 538–40.

58 See id.

59 Id at 538.

60 Id.

Justice William Brennan, joined by Justice Thurgood Marshall, filed a vigorous dissent in *Montoya de Hernandez*. Their main concern was the humiliating and degrading treatment that Montoya de Hernandez suffered during her detention.[61] They worried that the reasonable suspicion standard gave "sweeping and unmonitored authority" to low-level customs officials.[62] They were also interested in tethering the border search exception to its purpose. Though they believed that the need for wide-ranging detentions and searches for immigration and customs control was "unquestioned," they also thought that "far different considerations apply when detentions and searches are carried out for purposes of investigating suspected criminal activity."[63]

These dissenting justices drew a distinction that is, in some ways, parallel to limiting conditions that the Court has recognized in other lines of search cases that include exceptions to the warrant requirement. In *Arizona v Gant*,[64] the Court held that a vehicle search incident to arrest was proper only to the extent that it protected officer safety or was likely to produce "evidence relevant to the crime of arrest."[65] Officers were not permitted to go fishing for evidence of unrelated offenses. Similarly, the Court has held that roadblocks aimed at "general crime control" are usually impermissible, whereas those targeting specific criminal activity, such as drunk driving, are allowed.[66] Brennan could be seen as advocating for a similar standard in the border search context, requiring that the border search exception be tightly tethered to the aims of the border search doctrine: controlling "who and what may enter the country."[67]

C. Clarification of the Routine/Nonroutine Distinction: Protection of Privacy and Dignity Interests

Montoya de Hernandez established that certain types of nonroutine searches, such as detentions for sixteen hours and, potentially, body cavity and strip searches, require reasonable

---

61 See *Montoya de Hernandez*, 473 US at 545–48 (Brennan dissenting).

62 Id at 549 (Brennan dissenting).

63 Id at 554 (Brennan dissenting) (emphasis and citations omitted).

64 556 US 332 (2009).

65 Id at 343–44.

66 *Edmond*, 531 US at 47.

67 *Ramsey*, 431 US at 620. It is somewhat puzzling why the detection of illegal narcotics does not fall into the "immigration and customs control" rationales that Brennan and Marshall recognize as legitimate. *Montoya de Hernandez*, 473 US at 554 (Brennan dissenting).

suspicion. The boundaries of the category of nonroutine searches were very uncertain after that case, however, and the more recent case of *Flores-Montano* helps to clarify them.[68] Here, the search concerned the contents of a motor vehicle's gas tank. In the course of the search, the tank assembly was dismantled and drugs were discovered inside.[69] In holding that this search could be conducted absent reasonable suspicion, the Court focused on the types of Fourth Amendment interests that *Montoya de Hernandez* was meant to protect: the "dignity and privacy interests of the person being searched."[70] The Court explained that these interests, however, "simply do not carry over to vehicles."[71] In effect, the Court held that nonroutine searches are those that are highly intrusive to the dignity and privacy interests of those being searched, and *not* those that are merely unusual or require the extensive physical manipulation of the person's property.

This emphasis on privacy and dignity interests makes *Flores-Montano* an easy case. As the Court somewhat humorously noted, the petitioner's argument was that he had a "privacy interest in his fuel tank."[72] Though a fuel tank is not often open to public inspection, it is also not the sort of location that the Fourth Amendment is generally seen as protecting. Vehicles are not homes and are even less private than one's personal luggage. The vehicle-search exception cases are based, in part, on this recognition.[73] No private, intimate activity occurs in a car's gas tank, and no licit secrets are commonly stored there.

The innocent also have nothing to fear from a gas tank search.[74] As the Court noted, a gas tank should be solely a repository for fuel.[75] No great embarrassment or personal revelations are risked by subjecting it to search.[76] As Justice John Paul

---

68 See *Flores-Montano*, 541 US at 152.

69 Id at 151–52.

70 Id at 152.

71 Id.

72 *Flores-Montano*, 541 US at 154.

73 See *California v Acevedo*, 500 US 565, 569–71 (1991) (describing the vehicle-search exception).

74 For a case in which the Court has indicated that investigative methods that can reveal only criminal activity are less problematic, see *United States v Place*, 462 US 696, 707 (1983) (noting that drug-sniffing dogs reveal only contraband, thereby limiting the information that the government receives and the embarrassment and intrusion experienced by innocent property owners).

75 *Flores-Montano*, 541 US at 154.

76 Indeed, in the empirical survey, participants rated gas tank searches as among the least revealing of sensitive personal information. See text accompanying notes 199–203.

Stevens noted in *Montoya de Hernandez*, to allow a search without reasonable suspicion is to accept that a greater share of innocent people will be subjected to it.[77] Here, those innocent people would suffer inconvenience, but would not risk having their secrets publicly revealed or suffer any special humiliation.

The Court noted that some searches of property might be carried out in a "particularly offensive manner" or be "so destructive" that they should only be permitted given reasonable suspicion.[78] The gas tank search here, however, did not satisfy either requirement.[79] Therefore the search was routine and did not require elevated suspicion.

The question in the wake of *Flores-Montano* is whether the "dignity and privacy interests of the person being searched" ever require limitations on searches of property.[80] The Court's holding that these interests were insufficiently implicated by a vehicle search could be taken as a conclusion about searches of a specific type of property or as a general statement about all property searches.[81] Lower court judges trying to apply *Flores-Montano* to searches of electronic devices have differed on this point.[82]

II. BORDER SEARCHES AND ELECTRONIC DEVICES

Electronic devices pose novel challenges for the border search doctrine. If laptops are viewed as simply another good traveling across the border, then the doctrines of *Montoya de Hernandez* and *Flores-Montano* provide little support for requiring any elevated degree of suspicion for their search. Under *Flores-Montano* in particular, the Court seems to limit its concern about privacy and dignity interests to searches of *people*, not things,[83] and lower courts have traditionally treated searches of tangible property as routine and not requiring reasonable suspicion. For example, the Ninth Circuit has, at various times, upheld suspicionless searches of briefcases, purses and pockets, closed containers, and pictures and film.[84]

---

77 See *Montoya de Hernandez*, 473 US at 545 (Stevens concurring) (stating that even a requirement of reasonable suspicion will still allow for the search of many innocent people).

78 *Flores-Montano*, 541 US at 154 n 2, 155–56.

79 See id at 155–56.

80 Id at 152.

81 See id.

82 See notes 118–22 and accompanying text.

83 See *Flores-Montano*, 541 US at 155–56.

84 See notes 115–16 and accompanying text.

Yet a mobile electronic device is not like a gas tank. Though the gas tanks of innocent people contain few secrets (what secrets could they hide?), laptops and cell phones may contain office gossip, prescriptions for antidepressants, records of missed bill payments, political and religious tracts, and—not to forget the obvious—pornography. There is a reason why relationship-advice columnists often receive letters from men and women who snooped around the phones and computers of their spouses: there is much to find. Given this, are searches of mobile electronic devices sufficiently damaging that they implicate the same privacy and dignity interests that the Court sought to protect in *Montoya de Hernandez* and found lacking in *Flores-Montano*?

The Fourth and Ninth Circuits have adopted conflicting perspectives on this issue. While the Fourth Circuit has treated laptops like briefcases and luggage, which are generally subject to suspicionless searches, the Ninth Circuit has instead viewed them as sui generis, imposing a reasonable suspicion requirement for some searches.[85] In reaching these conflicting results, the circuits have disagreed about whether travelers understand that their devices can be searched at the border,[86] as well as whether laptop searches are sufficiently offensive to the privacy and dignity interests described in *Flores-Montano*.[87] The *Cotterman* court, as will be seen below, explicitly grounded its decision on its understanding of the answers to these questions.[88]

These questions are fundamentally empirical. Either travelers generally expect these searches, or they do not. Either they feel that their privacy and dignity interests are especially violated

---

85 Compare *United States v Ickes*, 393 F3d 501, 502 (4th Cir 2005) (holding that law-enforcement officials have broad powers to search property at the border), with *Cotterman*, 709 F3d at 966 (noting that "[r]easonable suspicion is a modest, workable standard" to apply to border searches of laptops).

86 Compare *Ickes*, 393 F3d at 506 (observing that an international traveler "should not be surprised" to have his property searched while crossing the border), with *Cotterman*, 709 F3d at 967 (observing that, while international travelers expect to have their belongings searched at the border, "they do not expect [ ] that, absent some particularized suspicion, agents will mine every last piece of data on their devices or deprive them of their most personal property for days").

87 Compare *Ickes*, 393 F3d at 506 (noting that a traveler's expectation of privacy "is substantially lessened" at the border), with *Cotterman*, 709 F3d at 966 (noting that "[a]n exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border").

88 *Cotterman*, 709 F3d at 967–68 (citing expectations, intrusiveness, and indignity as the reasons for its holding, and calling a laptop search a "substantial intrusion upon personal privacy and dignity").

by having their electronic devices searched, or they do not. There are also clear baselines against which the answers to these questions can be measured. Some searches, like strip searches, have been held to require reasonable suspicion.[89] Many other searches have not. The central question, then, is whether searches of electronic devices are seen as more like strip searches or more like pat-downs. As described below, courts are deeply divided on this issue.

A. The Fourth Circuit's Approach: Electronic Devices as Unexceptional

In the first federal appellate case in this area, *United States v Ickes*,[90] the Fourth Circuit did not require reasonable suspicion to justify the search of a computer at the Canadian border.[91] The questions before the court were whether the border search statute was broad enough to encompass electronic devices and whether there was a First Amendment exception for expressive materials.[92] In holding that the search statute in question (which mentioned "cargo" and "packages") was broad enough to cover electronic devices, the court noted the long history of border searches and the extremely broad latitude granted by the Supreme Court in past cases.[93] The *Ickes* court also rejected the argument that there should be a First Amendment exception for expressive materials.[94]

In explaining its decision, the court made an empirical claim about the expectations of travelers at the border. Specifically, it stated that searches were to be expected in this context. "When someone approaches a border, he should not be surprised that '[c]ustoms officers characteristically inspect luggage . . . ; it is an old practice and is intimately associated with excluding illegal articles from the country.'"[95] The court saw no reason why searches of electronic devices were less expected than any other type of search.

---

89 See notes 52–54 and accompanying text.

90 393 F3d 501 (4th Cir 2005).

91 See id at 505.

92 Id at 502. See also 19 USC § 1581(a) (permitting customs officials to investigate any "person, trunk, package, or cargo on board").

93 See *Ickes*, 393 F3d at 505–07.

94 See id at 506–07.

95 Id at 506, quoting *United States v Thirty-Seven Photographs*, 402 US 363, 376 (1971) (White) (plurality).

Though the court held that reasonable suspicion was not required, Judge J. Harvie Wilkinson argued that, "[a]s a practical matter, computer searches are most likely to occur where—as here—the traveler's conduct or the presence of other items in his possession suggest the need to search further."[96] He emphasized that customs officials simply do not have the resources to search every computer.[97] Thus, a high mechanical cost may diminish the need to also impose a legal barrier.

Importantly, there was no question in the *Ickes* case that reasonable suspicion was present. A routine search of Ickes's car at the border revealed "marijuana seeds, marijuana pipes, and a copy of a Virginia warrant for Ickes's arrest. [The officers] also found several albums containing photographs of provocatively posed prepubescent boys, most nude or semi-nude."[98] This alone would normally raise at least reasonable suspicion that child pornography would be present on Ickes's electronic devices.[99] There was, however, even more evidence. When asked, "Ickes admitted that stored on the computer were Russian videos of fourteen and fifteen year-old children engaged in sexual acts."[100] Though this case establishes that reasonable suspicion is not needed for the search of laptops and other electronic devices in the course of a border search, the agents in this case had not only reasonable suspicion and probable cause, but a freely given confession.

It is sometimes said that easy cases make bad law.[101] For the search in *Ickes* to be invalid, the Fourth Circuit would have needed to impose a warrant requirement for the search of expressive materials or hold that electronic devices were not covered in the border search statute. Neither holding could easily be supported by past precedent.[102] The outcome of *Ickes* was therefore in little doubt. Because the case would not have come out differently had the law required some elevated level of suspicion,

---

96 *Ickes*, 393 F3d at 507.

97 See id.

98 Id at 503.

99 Id at 507.

100 *Ickes*, 393 F3d at 503.

101 See, for example, Arthur R. Pearce, *Theft by False Promises*, 101 U Pa L Rev 967, 991 (1953) ("Thus do easy cases make bad law, for when it is obvious that a defendant is a criminal, it becomes less important how he is convicted, or of what crime.").

102 See *Ickes*, 393 F3d at 504–05 (observing that "the plain language of the [border search] statute authorizes expansive border searches"); id at 507 (noting the unlikelihood that the Supreme Court would create a First Amendment exception for the border search doctrine).

it is perhaps unsurprising that the court did not fully consider the merits of imposing a heightened standard. Absent from this decision is any discussion of the role of electronic devices in modern American life, or whether the amount of data held on electronic devices makes them qualitatively different than briefcases full of papers; the fact that the court chose not to address these arguments suggests that it rejected them. These factors, however, would prove central to the Ninth Circuit's consideration of electronic-device searches.

B. An Affirmation of *Ickes*: Laptops as Containers

Arguing before the Fourth Circuit, the defendant in *Ickes* warned that "any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer hard drive."[103] In ruling against him, Wilkinson wrote that "[t]his prediction seems far-fetched. Customs agents have neither the time nor the resources to search the contents of every computer."[104]

When the Ninth Circuit first addressed border searches of electronic devices, the case before it involved an apparently random search of an international air traveler's laptop.[105] Wilkinson was correct that customs agents do not have the resources to search *every* laptop, but he was mistaken if he believed that customs agents would not still search *some* laptops without cause. In *United States v Arnold*,[106] the agent began with a cursory examination of Arnold's laptop. "When the computer had booted up, its desktop displayed numerous icons and folders. Two folders were entitled 'Kodak Pictures' and one was entitled 'Kodak Memories.' [The agents] clicked on the Kodak folders, opened the files, and viewed the photos on Arnold's computer including one that depicted two nude women."[107] Though the government did not argue that these pictures depicted minors,[108] Arnold was nevertheless detained for several hours as his laptop was searched. The agents eventually found child pornography.[109]

---

103 Id at 506–07.

104 Id at 507.

105 *United States v Arnold*, 533 F3d 1003, 1005 (9th Cir 2008) (noting that the district court found that the search was random).

106 533 F3d 1003 (9th Cir 2008).

107 Id at 1005.

108 *United States v Arnold*, 454 F Supp 2d 999, 1001 & n 1 (CD Cal 2006).

109 *Arnold*, 533 F3d at 1005.

Though the Ninth Circuit would later adopt some measure of protection against laptop searches,[110] in this case it followed the Fourth Circuit's example, holding that the search did not require reasonable suspicion.[111] Foreshadowing the questions it would address in *Cotterman*,[112] however, the court in *Arnold* considered the argument that academic commentators often raise about laptop searches: that a laptop is "like the 'human mind' because of its ability to record ideas, e-mail, internet chats and web-surfing habits."[113] The defendant in *Arnold* attempted to analogize laptops to homes, particularly citing the number of personal documents likely to be stored on them and the number of secrets that could be revealed by searching them.[114] The court rejected these points, instead viewing laptops merely as closed containers. The court noted that "searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment."[115] Though laptops may contain substantial personal and expressive material, the court saw no reason to differentiate their search from any of the other searches that the Ninth Circuit had previously approved absent reasonable suspicion. These permissible searches included: "(1) the contents of a traveler's briefcase and luggage; (2) a traveler's 'purse, wallet, or pockets'; (3) papers found in containers such as pockets (allowing search without particularized suspicion of papers found in a shirt pocket); and (4) pictures, films and other graphic materials."[116]

Because laptops were not special in the eyes of the *Arnold* court, the analysis focused on a literal interpretation of the test for property searches that was endorsed by the Supreme Court in *Flores-Montano*.[117] A search of property could require reasonable suspicion if it either caused "exceptional damage to property" or was carried out in a "particularly offensive manner."[118] But neither exception applied here: the behavior of the customs agents

---

110 See Part II.C.

111 See *Arnold*, 533 F3d at 1008 ("Reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.").

112 See Part II.C.

113 *Arnold*, 533 F3d at 1006. For examples of such scholarly commentary, see notes 6, 18.

114 See *Arnold*, 533 F3d at 1006.

115 Id at 1007.

116 Id (citations omitted).

117 See Part I.C.

118 *Arnold*, 533 F3d at 1008–09.

appeared to have been professional, and the laptop itself was undamaged.[119]

Arguably, though, the Ninth Circuit missed the central point of the *Flores-Montano* holding. Consider again that *Flores-Montano* involved the search of a car's gas tank. The Supreme Court specifically noted that no private materials were likely to be stored in such a container and that the privacy and dignity interests of the searched party were not implicated by allowing a search of that area.[120] The same cannot be said of a laptop search.[121] This alternative interpretation of *Flores-Montano* was at the core of the district court's contrary ruling.[122]

C. The Ninth Circuit, Revisited

In a self-described "watershed case," the Ninth Circuit revisited the border search doctrine in *Cotterman*.[123] Cotterman was entering the United States from Mexico.[124] His name was flagged based on a fifteen-year-old conviction for child molestation and, with relatively minimal additional cause for suspicion, his laptop was searched.[125] The agents conducted a cursory examination of the laptop, as in *Arnold*, but initially found nothing of concern.[126] The laptop was then shipped almost 170 miles away and subjected to a comprehensive forensic examination.[127] Only then were images of child pornography discovered.[128] Initial analysis found seventy-five images of child pornography within the unallocated space of Cotterman's laptop.[129] Many of the images showed Cotterman sexually molesting children.[130] The court analyzed whether the escalation from a cursory examination at the border to a forensic examination off-site should have required

---

119 See id.

120 *Flores-Montano*, 541 US at 154–56.

121 See Part III.D.1.

122 See *Arnold*, 454 F Supp 2d at 1003–04 (noting that "[p]eople keep all types of personal information on computers" and that "opening and viewing confidential computer files implicates dignity and privacy interests").

123 *Cotterman*, 709 F3d at 956.

124 Id at 957.

125 See id at 957–58.

126 Id.

127 *Cotterman*, 709 F3d at 958.

128 Id.

129 Id.

130 Id at 959.

reasonable suspicion and whether reasonable suspicion was present.[131]

The majority's analysis in *Cotterman* stressed the limitations in the border search doctrine. Citing *Montoya de Hernandez*, the majority stated that "[e]ven at the border, individual privacy rights are not abandoned but '[b]alanced against the sovereign's interests.'"[132] Citing *Flores-Montano*, it emphasized the need to consider the "dignity and privacy interests of the person being searched," as well as the problems with searches of property that are destructive, particularly offensive, or overly intrusive as carried out.[133] Despite drawing on the same case law as the prior decisions, this choice of focus presented a starkly different picture of the border search doctrine.

The Ninth Circuit then adopted much the same reasoning that it had rejected in *Arnold*. It stated that a laptop search "directly implicat[es] substantial personal privacy interests. The private information individuals store on digital devices—their personal 'papers' in the words of the Constitution—stands in stark contrast to the generic and impersonal contents of a gas tank."[134] Drawing on original intent, the court noted the express listing of "papers" in the Fourth Amendment and explained that this "reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government."[135]

The court was also concerned about violating the expectations of ordinary travelers. It stated that "[i]nternational travelers certainly expect that their property will be searched at the border. What they do not expect is that, absent some particularized suspicion, agents will mine every last piece of data on their devices or deprive them of their most personal property for days."[136] As in *Ickes*,[137] the court here made an empirical claim about what ordinary people expect and assigned legal significance to its assumptions.

---

131 See *Cotterman*, 709 F3d at 957.

132 Id at 960, quoting *Montoya de Hernandez*, 473 US at 539.

133 *Cotterman*, 709 F3d at 963, quoting *Flores-Montano*, 541 US at 152.

134 *Cotterman*, 709 F3d at 964.

135 Id, quoting *United States v Seljan*, 547 F3d 993, 1014 (9th Cir 2008) (Kozinski dissenting). It is unclear why, if the listing of "papers" is of great importance, the listing of "effects" is not.

136 *Cotterman*, 709 F3d at 967.

137 See *Ickes*, 393 F3d at 506–07.

Despite tacitly adopting the *Arnold* defendant's take on the importance of electronic devices, the Ninth Circuit did not overrule that decision. It determined that "the legitimacy of the initial search of Cotterman's [laptop was] not in doubt."[138] Rather, only the "comprehensive and intrusive" forensic examination that followed triggered a reasonable suspicion requirement.[139] This was due to the especially intrusive nature of the forensic analysis. The majority likened it to "reading a diary line by line looking for mention of criminal activity—plus looking at everything the writer may have erased."[140] The court noted that:

> Computer forensic examination is a powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites. But while technology may have changed the expectation of privacy to some degree, it has not eviscerated it, and certainly not with respect to the gigabytes of data regularly maintained as private and confidential on digital devices.[141]

According to the court, this was "essentially a computer strip search. An exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border."[142]

This argument is similar to the concern raised in *Entick v Carrington*[143] and *Wilkes v Wood*[144] about the evils of giving officials wide discretion to search private papers (though those cases are not named in *Cotterman*).[145] The Fourth Amendment was created, in part, to prevent the state from having the power to conduct a general fishing expedition into a person's private papers

---

138 *Cotterman*, 709 F3d at 960.

139 Id at 962.

140 Id at 962–63.

141 Id at 957.

142 *Cotterman*, 709 F3d at 966.

143 95 Eng Rep 807, 817–18 (KB 1765) (holding that the monarchy's use of general warrants to search the plaintiff's private papers constituted trespass, "for papers are often the dearest property a man can have").

144 98 Eng Rep 489, 498 (KB 1763) (noting that if the state is empowered to use general warrants to seize private property without specifying what property has been taken, or even a suspect's name, that power "is totally subversive of the liberty of the subject").

145 See Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 Suffolk U L Rev 53, 65–67 (1996) (describing how the Fourth Amendment was in part a response to the excesses of general warrants in the English cases of *Entick* and *Wilkes*).

and effects.[146] In the eyes of the majority, this extensive border search eviscerated the target's privacy interests.[147]

1. Adapting doctrine to account for changes in technology.

The *Cotterman* court believed that existing border search doctrine needed to be updated to account for the effects of changes in technology.[148] As support for this type of doctrinal tailoring, the court cited *Kyllo v United States*,[149] which held that government monitoring of a home's heat signature is a search within the meaning of the Fourth Amendment.[150] Prior to the development of thermal-imaging devices, no one would have thought that monitoring heat would amount to a privacy violation. Given what technology had made possible by the beginning of the twenty-first century, however, such signals could be used to peer within the private space of the home. The majority in *Cotterman* believed that this presented a parallel case: the intrusiveness of a search of one's traveling possessions had previously been small but, with the rise of mobile computing, had increased substantially.[151]

First, the majority was concerned with the sheer amount of information carried.[152] Though a person might select a few files out of a cabinet to carry in a briefcase, the laptop carries the entire filing cabinet, if not the entire office. This contributes to the further problem that one does not select the files that one carries on a laptop in the same way that one selects the papers that one puts in a briefcase. This is particularly worrisome in cases in which deleted files are recovered. Then it becomes prohibitively difficult to *not* carry a file if one does not have the resources to have a separate traveling laptop or phone. People therefore often cannot make meaningful decisions about what they are exposing to potential search.[153]

The type of information involved in electronic-device searches also presented a problem. The majority referred to "[l]aptop computers, iPads and the like" as being "simultaneously offices

---

146 See id. See also generally James Otis, *Against the Writs of Assistance* (1761), in Melvin I. Urofsky and Paul Finkelman, eds, *Documents of American Constitutional & Legal History Volume I: From the Founding to 1896* 38 (Oxford 3d ed 2008).

147 See *Cotterman*, 709 F3d at 957.

148 See id at 956–57.

149 533 US 27 (2001).

150 Id at 40.

151 See *Cotterman*, 709 F3d at 965.

152 See id at 964.

153 See id at 965.

and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails."[154] In short, highly revealing and embarrassing information. This is far beyond what would normally be found in a briefcase.[155] The Supreme Court recently recognized the force of this argument in *Riley*, noting that cell phones often contain "a broad array of private information never found in a home in any form—unless the phone is."[156]

Though it was not at issue in this case, the *Cotterman* court also commented on a problem that often arises in cell phone searches. One common use of laptops and smartphones is to access data stored "in the cloud." For example, consider one's Gmail account. Comparatively little data related to the account is stored on the computer itself; most is on Google's servers. But the laptop or smartphone is a "key" to the file store. The *Cotterman* court described using a mobile electronic device as "akin to the key to a safe deposit box."[157] This raises two problems. First is the aforementioned issue of choosing the files that one brings. If one's laptop has been used to access Google, Amazon, Facebook, and the like, it may be possible to recover those passwords with a forensic examination. The potential for privacy intrusion is therefore vast.

A further problem with searches of data in the cloud is that the "virtual safe deposit box" does not itself cross the border. Though from the customs agent's perspective he has merely tapped the mail icon on a traveler's phone, he has actually asked the phone to communicate with servers located all over the world.[158] Customs agents searching smartphones apparently regularly open apps,[159] so this is not a purely academic concern.

Because "[s]uch a thorough and detailed search of the most intimate details of one's life is a substantial intrusion

---

154 Id at 964.

155 Participants in this Comment's survey believe that more would be exposed by search of their personal electronic devices than by searches of their other luggage. See Table 2.

156 *Riley*, No 13-132, slip op at 21.

157 *Cotterman*, 709 F3d at 965.

158 See id.

159 See *Abidor v Napolitano*, 2013 WL 6912654, *15–19 (EDNY) (holding that customs agents had reasonable suspicion to search the personal computer files of an Islamic studies graduate student whose laptop contained images of terrorist-organization rallies). See also Patrick E. Corbett, *The Future of the Fourth Amendment in a Digital Evidence Context: Where Would the Supreme Court Draw the Electronic Line at the International Border?*, 81 Miss L J 1263, 1266–68 (2012) (describing the *Abidor* case).

upon personal privacy and dignity," the *Cotterman* court held that a showing of reasonable suspicion was necessary in the context of forensic examinations of computers, calling it "a modest requirement in light of the Fourth Amendment."[160]

2. In the concurrence and dissent, endorsements of *Ickes*.

Judges Consuelo Callahan and Milan Smith wrote strong opinions that took issue with the new reasonable suspicion requirement. Callahan concurred in the judgment—the majority found reasonable suspicion and held that the evidence was admissible—but sharply disagreed with requiring elevated suspicion for any search of an electronic device at the border.[161] Smith dissented because he would have held that the search amounted to an "extended border search," which would require reasonable suspicion regardless of what was being searched, and he did not think that reasonable suspicion was present here.[162] Despite disagreeing on the appropriate disposition of the case, both judges raised the same types of concerns about the new reasonable suspicion rule. Callahan focused on the "person" language from *Flores-Montano*, stating that highly intrusive searches of things should not require reasonable suspicion unless they are either destructive or offensively conducted.[163] Smith similarly would have held that reasonable suspicion should be required at the border only for "highly intrusive searches *of the person*" and searches of property that are destructive or carried out in an offensive manner.[164] In adopting this interpretation, Callahan and Smith revisited the now-familiar tension over the meaning of *Flores-Montano*: Are the dignity and privacy interests that make some searches of the body worrisome *never* implicated in searches of property, or were they merely not implicated in that case's search of a gas tank?

Smith also attacked the majority's main premise that computers are intensely private. He pointed out that people regularly

---

160 *Cotterman*, 709 F3d at 968.

161 See id at 971 (Callahan concurring in part, dissenting in part, and concurring in the judgment).

162 Id at 989 (Smith dissenting). Smith's dissent also pointed out that the majority had to make some fairly convoluted assumptions to find reasonable suspicion in this case. See id at 990–93 (Smith dissenting). Again, it should be remembered that the class of defendants bringing these computer-search cases is typically highly unsympathetic.

163 See id at 973 (Callahan concurring in part, dissenting in part, and concurring in the judgment).

164 *Cotterman*, 709 F3d at 982 (Smith dissenting).

share sensitive personal information on the Internet, arguing that, "[i]ronically, the majority creates a zone of privacy in electronic devices at the border that is potentially greater than that afforded the Google searches we perform in our own homes, and elsewhere."[165] If people take no pains to keep online activity private from Google, why should searches by customs agents be limited? Callahan was similarly unconcerned. To her, "electronic devices are like any other container" and should be subject to search on the same grounds.[166]

Both Smith and Callahan also specifically rejected the argument that the quantity of data stored in electronic devices should change the analysis. According to Smith, "The documents carried on today's smart phones and laptops are different only in form, but not in substance, from yesterday's papers, carried in briefcases and wallets."[167] And "[u]nder the majority's reasoning, the mere process of digitalizing our diaries and work documents somehow increases the 'sensitive nature' of the data therein, providing travelers with a greater expectation of privacy in a diary that happens to be produced on an iPad rather than a legal pad."[168] The majority argued that size mattered, increasing the magnitude of the privacy invasion, but Callahan and Smith saw no basis in the doctrine for that conclusion.[169]

D. The State of the Law

To date, it appears that no defendant challenging a border search of an electronic device has ever won suppression based on a lack of reasonable suspicion.[170] Some courts have explicitly held reasonable suspicion irrelevant to the more routine computer

---

165 Id at 986 (Smith dissenting) (noting that 500 million people are members of Facebook and that Internet cookies, which track browsing activity, are ubiquitous).

166 Id at 976 (Callahan concurring in part, dissenting in part, and concurring in the judgment).

167 Id at 987 (Smith dissenting). Callahan expressed a similar sentiment. See id at 977–78 (Callahan concurring in part, dissenting in part, and concurring in the judgment).

168 *Cotterman*, 709 F3d at 987 (Smith dissenting) (emphasis omitted).

169 See id (Smith dissenting); id at 977–78 (Callahan concurring in part, dissenting in part, and concurring in the judgment).

170 See Corbett, 81 Miss L J at 1269–74 (cited in note 159). In his review of lower and appellate court decisions on border searches of electronic devices, Professor Patrick Corbett finds fifteen cases, fourteen of which concern child pornography, which were decided over a five-year period. The only appellate case described, apart from the Fourth and Ninth Circuit decisions, is *United States v Irving*, 452 F3d 110 (2d Cir 2006). In that case, the court did not decide whether a search of 3.5-inch computer disks was routine or nonroutine because the search was supported by reasonable suspicion. See id at 124.

searches at issue in particular cases.[171] Others have found reasonable suspicion and not determined whether it was necessary.[172]

This does not appear to have changed in the brief time since the *Cotterman* decision. In an extremely short opinion, one lower court held that, even if it were inclined to adopt *Cotterman*'s reasonable suspicion requirement, the search before it was not comprehensive and intrusive enough to trigger it.[173] A more extensive and much-anticipated opinion in *Abidor v Napolitano*[174] reached a similar result, holding that reasonable suspicion was present, rendering moot the question whether it was required.[175] That case concerned a challenge to Department of Homeland Security directives that authorize the search of electronic devices at border crossings.[176] In reaching its conclusion, the court emphasized that travelers know that their electronic devices are at risk of both search and theft and therefore would be wise to choose carefully what files they carry with them.[177]

The most important recent development in this area is the Supreme Court's decision in *Riley*, which was strongly protective of individuals' privacy interests in electronic devices in the context of searches incident to arrest.[178] That opinion did not directly discuss border searches, but it is extremely likely that the next round of border cases will grapple with the Court's willingness to write special rules for electronic devices in the arrest context. Given that border search doctrine is ripe for reevaluation, the persuasiveness of the border-specific elements of the *Cotterman* analysis is of immediate importance.

---

171 See, for example, *United States v Stewart*, 729 F3d 517, 521–24 (6th Cir 2013) (holding that a reasonable suspicion inquiry is inapplicable to a laptop search that involved using the image-preview function to view thumbnails of photographs).

172 See, for example, *United States v Rogozin*, 2010 WL 4628520, *3–4 (WDNY) (determining that reasonable suspicion was present because the accused avoided eye contact during the interview with a border agent and had a questionable itinerary); *United States v Verma*, 2010 WL 1427261, *4 (SD Tex) (noting that the investigating agents possessed "the requisite particularized and objective basis" to have reasonable suspicion of Verma's wrongdoing).

173 See *United States v Wallace*, 2013 WL 1702791, *1 (ND Ga) (noting that the intrusion in the instant case was not as intrusive as the search in *Cotterman*).

174 2013 WL 6912654 (EDNY).

175 See id at *18.

176 Id at *1.

177 See id at *13–14.

178 See *Riley*, No 13-132, slip op at 17–21.

III. AN EMPIRICAL STUDY OF LAY ATTITUDES AND EXPECTATIONS

As shown in Part II, courts have speculated about the role of electronic devices in daily life, the kinds of treatment that citizens expect when crossing the national border, and the degree of intrusion represented by searches of electronic devices. Consistent with the instruction in *Flores-Montano* to consider the privacy and dignity interests of the person being searched,[179] courts have, in part, based their rulings on these impressions.[180] But none of these cases, and little of the secondary literature, has cited empirical data on citizens' privacy expectations and the degree of intrusion caused by searches of electronic devices. In the absence of empirical data, judges have had to guess at the background social facts even though those facts are highly relevant to their decisions. As was seen in the argument between the majority and the dissent in *Cotterman* about the degree of security that individuals have and expect in their electronic communications,[181] not all judges have arrived at the same set of answers. As judges and justices are now weighing whether to follow the *Cotterman* court in treating electronic devices as special, it would be helpful to determine how much everyday people know about searches of electronic devices and how they feel about those searches.

A. Past Work on the Perceived Intrusiveness of Searches

There is a limited amount of prior empirical work analyzing privacy attitudes in the context of police searches, much of it by Professors Christopher Slobogin and Joseph Schumacher. In the early 1990s, Slobogin and Schumacher conducted a survey asking a sample of students to rate the perceived intrusiveness of various types of searches drawn from controversial Fourth Amendment cases.[182] They found that a body cavity search (conducted at the border) was judged to be the most intrusive. A search of a bedroom, reading a personal diary, and monitoring a

---

179 See *Flores-Montano*, 541 US at 152.

180 See notes 85–87 and accompanying text.

181 See *Cotterman*, 709 F3d at 986 (Smith dissenting) (commenting that individuals regularly convey to Google the very sensitive personal information that is at issue in electronic searches).

182 Christopher Slobogin and Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 Duke L J 727, 737 (1993).

phone for thirty days were seen as only slightly less intrusive.[183] Unfortunately, the researchers included only two border scenarios, the body cavity search and a pat-down, and—as is to be expected given that the paper was published in 1993—did not probe attitudes toward the search of personal computers.[184]

This study was recently replicated by Professor Jeremy Blumenthal, Doctor Meera Adya, and Jacqueline Mogle.[185] Their results largely tracked those of Slobogin and Schumacher, with some minor differences. They found, for example, that reading a personal diary was now perceived to be the most intrusive search, and that perusing bank records, tapping a corporation's computer network, and searching a bedroom were all *more* intrusive than the body cavity search.[186] The scenarios used in this study were the same as in Slobogin and Schumacher's study, so they do not bear specifically on border searches of mobile electronic devices. The results are suggestive, however. They show that people can plausibly be expected to view searches of electronic devices as being as intrusive as body cavity and strip searches—the kinds of searches that *Montoya de Hernandez* suggested would likely require elevated suspicion.[187] Consider the personal diary example. Like the mobile electronic device, a diary can be searched without harm to it or physical contact with the person. But, again like the mobile device, searching a diary could reveal the most intimate secrets of the person.

These studies have some shared limitations. Though some of the scenarios are suggestive of views toward searches of electronic devices, no scenario is closely on point. The studies also used samples of students, and even the more recent of the studies used the same search scenarios that were written for the 1993 survey. The dependent measure was also somewhat limited. Slobogin and Schumacher had their participants rate "intrusiveness,"[188] and the replication study followed their example.[189] Professor Orin Kerr has argued that this is not the best term. He believes that the term "intrusive suggests interference with

---

183 See id at 738–39.

184 See id.

185 See Jeremy A. Blumenthal, Meera Adya, and Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U Pa J Const L 331, 341–43 (2009).

186 See id at 359.

187 See text accompanying notes 53–54.

188 Slobogin and Schumacher, 42 Duke L J at 735–37 (cited in note 182).

189 See Blumenthal, Adya, and Mogle, 11 U Pa J Const L at 345 (cited in note 185).

the status quo. The more intrusive something is, the more it alters the world that existed before. As a result, police techniques that are common, are expected, or go unnoticed will tend to seem unintrusive."[190] Similarly, that which is uncommon or unexpected will seem more intrusive. But merely because something is uncommon does not mean that it violates civil liberties (and merely because it is common does not mean that it does not).[191] Because of this concern, I employ a wider range of dependent measures.

B. Participants

A sample of 300 adults living in the United States was recruited from Amazon's Mechanical Turk service.[192] The resulting set of respondents was diverse, if not representatively weighted. Ten participants were excluded for having completion times that were less than half that of the median participant, and a further five were eliminated because they reported that they were not US citizens, leaving 285 participants. Of the remaining sample, the median age was 35 (range 18–74, M = 37.56, SD = 12.77). 54.7 percent of the sample was female, 46.7 percent held a valid passport, and 71.6 percent had traveled outside the United States at some point. According to the State Department, in 2013 there were 117.4 million passports in circulation for 316.1 million Americans (37.2 percent),[193] making the sample more travel ready than the national population as a whole. The sample was also somewhat better educated, with a greater proportion of participants holding four-year college degrees.[194] 85.6 percent of

---

[190] Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 Mich L Rev 951, 958 (2009).

[191] See id at 959.

[192] For a description of Mechanical Turk's use as a data-collection tool, see generally Michael Buhrmester, Tracy Kwang, and Samuel D. Gosling, *Amazon's Mechanical Turk: A New Source of Inexpensive, yet High-Quality, Data?*, 6 Persp Psychological Sci 3 (2011). It is commonly used in the social sciences and in law as a means of low-cost data collection. See, for example, David A. Hoffman and Tess Wilkinson-Ryan, *The Psychology of Contract Precautions*, 80 U Chi L Rev 395, 410 (2013); Stuart P. Green and Matthew B. Kugler, *Public Perceptions of White Collar Crime Culpability: Bribery, Perjury, and Fraud*, 75 L & Contemp Probs 33, 42 (2012).

[193] Bureau of Consular Affairs, *Valid Passports in Circulation (1989–Present)*, online at http://travel.state.gov/content/passports/english/passports/statistics.html (visited Aug 12, 2014); US Census Bureau, *State & County QuickFacts* (Mar 27, 2014), online at http://quickfacts.census.gov/qfd/states/00000.html (visited Aug 12, 2014).

[194] In the sample, 12.6 percent of participants had graduate degrees, 36.8 percent had four-year college degrees, 20.4 percent had two-year degrees, 28.8 percent had high school degrees, and 1.4 percent had not completed high school. According to the US Census Bureau, 13.5 percent of those aged 35–39 have graduate degrees, a further 22.5 percent

the sample identified as white, 6.7 percent was black, and 5.3 percent was South or East Asian.

C. Types of Searches

Each participant was asked to evaluate twenty-six different types of searches. Thirteen of the described searches involved electronic devices and thirteen did not. The searches without electronic devices were presented first, in random order. Then the electronic searches were presented, again in random order. The searches were presented in the following form:

"When a person is seeking to enter the United States, whether it is at an airport or a land crossing, imagine a border agent wanted to: [one of the below was inserted here]"

- Ask the traveler to fill out a customs form asking them to state all the major purchases abroad that they are trying to bring back into the country.
- Ask the traveler where they have been traveling and what they did there.
- Fingerprint the traveler.
- Have a drug-sniffing dog walk around the traveler's car.*[195]
- Open the traveler's briefcase or backpack and read any papers that might be inside.
- Open the traveler's briefcase or backpack to check whether it contains drugs, but not to read any papers that might be inside.
- Pat down the traveler.
- Perform a body cavity search on the traveler.
- Put the traveler's car up on a jack and check the gas tank for contraband.*
- Read the traveler's diary, found in their shoulder bag.
- Search the traveler's car for any packages they might be carrying and open the packages.*
- Strip search the traveler.

---

have four-year degrees, 10.5 percent have two-year degrees, 42.2 percent have a high school degree but have not completed any college degree, and 11.3 percent do not have a high school degree. See US Census Bureau, *Educational Attainment in the United States: 2013 – Detailed Tables*, online at http://www.census.gov/hhes/socdemo/education/data/cps/2013/tables.html (visited Aug 12, 2014).

[195] For those scenarios marked with an asterisk, the text asked participants to picture only a land crossing instead of an airport or land crossing.

- Take the traveler's car to a location 90 minutes away and have a drug-sniffing dog walk around it.*

"The following questions concern the search of various electronic devices, such as cellphones, laptops, and tablets. When a person is seeking to enter the United States, whether it is at an airport or a land crossing, imagine a border agent wanted to: [one of the below was inserted here]"[196]

- Dismantle the traveler's device to inspect the inside, assuming that it can be reassembled without damage.
- Power on the traveler's device.
- Review the traveler's most recently opened documents and applications.
- Search the traveler's device for a list of most recent calls.
- Search the traveler's device for the 10 most recent text messages.
- Search the traveler's device's browser for a list of recent searches.
- Search the traveler's entire picture archive.
- Search the traveler's entire text message history.
- Subject the traveler's device to a forensic examination to recover any files that the traveler may have deleted, including pictures, documents, and emails.
- Use the traveler's device to access the traveler's email account and search their emails.
- Use the traveler's device to log on to the traveler's Facebook account.
- Use the traveler's device to read the traveler's electronic diary.
- Use the traveler's device's saved passwords to log on to other websites, like Amazon or eBay, to examine recent purchases.

D. Procedures and Results

After agreeing to participate in the study, respondents were told that they would be asked to evaluate a series of searches occurring at the national border. Before rating any searches, participants were also told that:

---

[196] Other than the preamble, this is the same prompt as before.

> Whether they are a citizen returning from abroad or a tourist from another country, a person can be searched when they cross the border into the United States. . . . Some [search] methods can be used on any traveler, regardless of whether they have done anything to make the border guards suspicious. Others can only be used if the traveler seems shifty or appears to be hiding something.

For each of the twenty-six searches in the study, participants were asked four questions. The first three questions, answered on scales ranging from 0 (not at all) to 100 (very), asked participants to rate how intrusive the search was (mirroring Slobogin and Schumacher), how likely the search was to reveal sensitive personal information, and how embarrassing the search would be. The two new questions were intended to address the privacy and dignity concerns, respectively, that were cited in *Flores-Montano*.[197] The final question for each search asked participants whether the government could conduct this search on "any traveler they choose," "[o]nly if they can give a particular reason to suspect the specific traveler of criminal activity" (intended to capture the meaning of reasonable suspicion), or "[o]nly if they have a warrant from a judge."[198]

1. Intrusiveness, sensitive information, embarrassment, and expectations.

Data on each of the three continuous measures were analyzed using within-subjects ANOVAs with Bonferroni-corrected pairwise comparisons.[199] The results are presented in Table 1. The most severe of the electronic searches are seen as nearly as intrusive as body cavity and strip searches. Five electronic searches, including the forensic analysis from *Cotterman* and the reading of an entire text message archive, are seen as significantly more intrusive than all of the traditional searches other than those two body searches. Every electronic search that

---

197 See *Flores-Montano*, 541 US at 152.

198 At the very end of the study, participants were also invited to make free-response comments. The second epigraph is from that inquiry.

199 To avoid a multiple-comparison issue, Bonferroni corrections were used for the pairwise tests. This highly conservative choice likely obscures some meaningful differences among the scenarios. Null effects should be interpreted with caution.

Unsurprisingly, scores on each of the three measures differed significantly across scenarios. Intrusiveness: $F(25, 3131.50) = 353.08$, $p < .001$ $\eta^2 = .55$; Reveal information: $F(25, 2894.55) = 219.79$, $p < .001$ $\eta^2 = .44$; $F(25, 3534.69) = 248.44$, $p < .001$ $\eta^2 = .47$. Due to sphericity violations, Greenhouse-Geisser corrections were used for all three analyses.

accessed the contents of the device was seen as significantly more intrusive than reading the papers in a traveler's briefcase—the analogy drawn in the *Cotterman* dissent.[200] All electronic searches, except merely turning the device on, were seen as more intrusive than the search of the inside of a car's gas tank (which does not require reasonable suspicion under *Flores-Montano*[201]). Effectively, the electronic searches divide into those that are like a body cavity search, those that are like reading a person's personal diary, and those that are like the ninety-minute–drug-dog sniff search at issue in *United States v Place*.[202] The single exception is turning the device on to see whether it works.

The four searches seen as most revealing of private information all involve electronic devices. If we set aside reading one's (physical) diary as being somewhat sui generis, the top ten most revealing searches are all of one's electronic devices.

The embarrassment ratings are consistent with the other two measures. As one might expect, the body cavity and strip searches are clearly distinct from all other possible searches. Following these, however, are reading a person's personal diary and a range of electronic searches (of the e-mail account, the text archive, the deleted files, and the picture archive), all of which are statistically and practically impossible to distinguish from one another. The list of recent calls is the least embarrassing of the content-related electronic searches.

Though greatly concerned about the embarrassment and privacy violation of electronic-device searches, ordinary citizens appear to believe that they are protected from them, even at border crossings. In *Cotterman*, the Ninth Circuit worried that forensic analysis of electronic devices would violate the expectations of travelers, while the Fourth Circuit in *Ickes* believed that travelers would not be surprised.[203] The judges in *Cotterman* were more correct than they likely realized. For the majority of electronic searches, including those that even the *Cotterman* court would have considered routine, less than 11 percent of participants believed that border agents could conduct the search without at least some articulable suspicion. For *only*

---

[200] See *Cotterman*, 709 F3d at 987 (Smith dissenting).

[201] See *Flores-Montano*, 541 US at 155–56.

[202] 462 US 696, 709 (1983) (holding that a ninety-minute detention to allow for a drug-dog sniff search exceeded the permissible limits of a *Terry* stop).

[203] Compare *Cotterman*, 709 F3d at 967, with *Ickes*, 393 F3d at 506.

one content-related electronic search did a majority of participants believe that the search could be conducted without a warrant from a judge. For that single exception—a search of the recent call list—49.47 percent of participants still believed that a warrant was required. Interestingly, the overwhelming majority of participants recognized that the most commonly used search techniques (pat-down, questioning about travel plans, drug-sniffing dogs, and opening luggage) could be conducted on any traveler even without articulable cause. The views of the participants therefore track reality to a substantial degree in the context of traditional searches. Also interesting is that searching the inside of a gas tank was believed to require reasonable suspicion but not a warrant, contra the decision in *Flores-Montano* holding that reasonable suspicion was not required.

Consider the reasonable suspicion standard in the context of these data. Were content-related searches of electronic devices to be permitted absent reasonable suspicion, this policy would allow without-cause searches that (1) are seen as among the most intrusive contemplated or recorded in the current case law, (2) are the *most* revealing of sensitive information, (3) are only less embarrassing than strip searches and body cavity searches, and (4) would surprise more than 85 percent of respondents. In terms of the *Flores-Montano* dignity and privacy criteria, this would be a perverse result.

TABLE 1A. RATINGS OF TRADITIONAL SEARCHES, SORTED BY PERCEIVED INTRUSIVENESS

N = 285

Search Type	Intrusiveness	Reveals Sensitive Info	Embarrassing	Expected Standard: Any Traveler	Expected Standard: Reasonable Suspicion	Expected Standard: Warrant
Body Cavity	95.97_{a} (12.36)	64.66_{hi} (35.47)	96.44_{a} (12.63)	9%	47%	43%
Strip	94.85_{ab} (14.76)	70.79_{fg} (33.26)	96.31_{a} (11.68)	12%	52%	36%
Read Diary	87.56_{fg} (18.49)	83.61_{bcd} (25.22)	83.14_{b} (23.76)	21%	29%	49%
90-min Drug Dog	81.58_{hi} (25.18)	46.23_{k} (33.40)	61.84_{efg} (34.47)	12%	39%	48%
Read Papers in Bag	75.28_{ij} (24.62)	73.36_{fg} (26.73)	62.94_{ef} (29.07)	33%	35%	32%
Search Car/Open Packages	70.13_{jk} (24.74)	60.95_{ij} (29.59)	55.95_{gh} (30.81)	36%	49%	15%
Inside Gas Tank	65.28_{kl} (29.03)	32.51_{mn} (30.01)	51.46_{hi} (34.07)	21%	62%	17%
Pat-Down	59.46_{l} (29.10)	39.42_{l} (30.62)	56.32_{fgh} (33.56)	68%	29%	2%
Fingerprint	58.18_{lm} (34.03)	53.76_{jk} (35.52)	43.53_{ij} (36.58)	38%	36%	25%
Open Bag/Don't Read Papers	50.07_{mn} (29.33)	47.13_{k} (31.84)	39.91_{l} (32.04)	70%	27%	3%
Drug Dog	31.48_{o} (31.60)	30.93_{mn} (30.95)	31.38_{k} (33.06)	76%	20%	5%
Customs Forms	31.15_{o} (28.88)	34.96_{lm} (30.29)	22.09_{l} (26.93)	82%	15%	3%
Ask about Travel	26.89_{o} (27.66)	27.70_{n} (26.76)	17.48_{l} (24.28)	88%	11%	1%

TABLE 1B. RATINGS OF ELECTRONIC SEARCHES, SORTED BY PERCEIVED INTRUSIVENESS

N = 285				Expected Standard		
Search Type	Intrusiveness	Reveals Sensitive Info	Embarrassing	Any Traveler	Reasonable Suspicion	Warrant
Forensic Deleted Files	94.08_{abc} (11.95)	89.01_{a} (20.57)	81.72_{b} (25.83)	8%	14%	78%
E-mail Account	93.10_{abc} (13.93)	87.58_{ab} (21.35)	80.60_{b} (25.88)	9%	21%	71%
Entire Texts	92.91_{abcd} (13.37)	86.85_{abc} (21.56)	81.94_{b} (25.26)	10%	23%	67%
Amazon/eBay/Other	92.20_{bcde} (14.56)	82.71_{cd} (26.08)	71.85_{d} (30.91)	8%	20%	72%
Electronic Diary	91.93_{bcde} (14.82)	86.69_{abcd} (21.76)	82.53_{b} (24.49)	11%	24%	65%
Picture Archive	90.39_{ef} (16.05)	79.61_{de} (27.31)	79.23_{bc} (26.08)	10%	32%	58%
Facebook	90.14_{ef} (16.77)	81.76_{d} (26.49)	75.06_{cd} (28.40)	11%	26%	63%
Recent Texts	86.89_{g} (17.95)	77.10_{ef} (25.92)	72.67_{d} (28.49)	9%	36%	54%
Recent Web Searches	86.04_{gh} (18.42)	76.89_{ef} (26.74)	72.58_{d} (29.53)	10%	38%	51%
Recent Docs and Apps	84.93_{gh} (19.99)	76.32_{ef} (26.42)	66.57_{e} (31.48)	14%	32%	54%
Recent Calls	84.31_{gh} (19.43)	70.69_{gh} (28.01)	61.53_{defg} (31.38)	13%	38%	49%
Dismantle/Reassemble	80.90_{hi} (24.65)	49.58_{k} (37.22)	56.43_{fgh} (35.05)	16%	44%	39%
Power On	48.60_{n} (33.64)	37.33_{lm} (32.90)	35.40_{jk} (33.63)	49%	35%	16%

Note: For Tables 1a and 1b, means are reported with standard deviations in parentheses. Means within a column across both tables that share a subscript are not significantly different from one another. For example, a search of a Facebook account (ef) is significantly more intrusive than searches of recent texts (g) or of a gas tank (kl), but it is not significantly less intrusive than a search of an electronic diary (bcde) because both share a subscript (e).

2. Extent of revelation.

When considering whether the contents of electronic devices should be protected from searches, courts may want to know what types of information such searches are likely to reveal. Particularly, they may wish to know what types of information are revealed to a greater extent by searches of electronic devices than by more traditional searches. After completing their ratings of the various searches, participants were therefore asked to think about the types of information available on their electronic devices. They were given a list of information types and, for each, were asked to check whether that type of information could be found on their device. These types of information were: recent purchases, banking information, information about the personal lives of friends and family, romantic interests or sex life, interest in pornography, credit history, income level, ideological beliefs, educational records, sensitive medical information, and medical prescriptions. Participants were then asked to think about the other things that they travel with and to rate how much someone searching their electronic devices would learn on a scale from 1 ("[n]o more than from my other possessions") to 5 ("[m]uch more than from my other possessions") about each information type.

TABLE 2. WHETHER MORE CAN BE LEARNED FROM THE SEARCH OF THE TRAVELER'S ELECTRONIC DEVICES THAN FROM OTHER POSSESSIONS

Type of Information	Info Present	Learn How Much More from Electronic Search?	
Recent Purchases	82%	3.58 (1.46)	$t(284)=29.87^{***}$
Banking	76%	3.41 (1.56)	$t(284)=26.09^{***}$
Family Information	76%	3.51 (1.41)	$t(284)=29.93^{***}$
Romantic Life	55%	2.89 (1.56)	$t(283)=20.49^{***}$
Pornography	45%	2.59 (1.71)	$t(282)=15.59^{***}$
Credit	42%	2.63 (1.58)	$t(282)=17.39^{***}$
Income	41%	2.60 (1.45)	$t(283)=18.52^{***}$
Ideology	40%	2.53 (1.46)	$t(282)=17.60^{***}$
Educational Records	35%	2.35 (1.48)	$t(284)=15.36^{***}$
Medical	28%	1.98 (1.35)	$t(283)=12.23^{***}$
Prescriptions	24%	1.93 (1.37)	$t(284)=11.43^{***}$

$^{*}p < .05$; $^{**}p < .01$; $^{***}p < .001$

Participants reported that a search of their electronic devices would yield more information about all of the topic domains than would a search of their other belongings. Generally, participants felt that their electronic devices would be most revealing of their recent purchases, banking, and information about family and friends, but also believed that their romantic lives and interests in pornography could be exposed.

3. Correlates of privacy concern.

An additional question concerns the demographic and ideological correlates of privacy concern in the context of border searches. Is concern about border searches concentrated among particular subsets of the population, or is it felt equally across different demographic groups? The survey instrument included a number of items intended to address this topic. Participants were asked to report their age and educational attainment as part of their demographic information.[204] They also rated how liberal or conservative they are—(1) overall, (2) on economic issues, and (3) on social issues—on a scale ranging from 1 ("Very Liberal") to 7 ("Very Conservative").

It is also interesting to analyze whether those concerned about searches of electronic devices at the border are concerned with privacy more generally. The study therefore included a measure of consumer-informational privacy concern that was commonly used by Professor Alan Westin.[205] Participants rated how much they agreed or disagreed with three statements on a scale ranging from 1 ("Disagree Very Strongly") to 4 ("Agree Very Strongly"). The statements were: (1) Consumers have lost all control over how personal information is collected and used by companies; (2) Most businesses handle the personal information they collect about consumers in a proper and confidential way (reverse scored); and (3) Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today (reverse scored).[206] I averaged the items to create a composite (α = .72) coded so that higher scores indicated greater privacy concern.

---

[204] For the sample's distributions on these, see text accompanying notes 192–93.

[205] For an overview of Westin's work, see Ponnurangam Kumaraguru and Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin's Studies* *5–16 (Institute for Software Research International, Dec 2005), online at http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf (visited Aug 12, 2014).

[206] See id at *13.

As with the Westin-privacy-concern questions, it was also desirable to create composite scores for the different types of searches. There was no reason to believe that the factors underlying privacy concerns about e-mail would be fundamentally different than the factors underlying privacy concerns about text messages, for example. The searches were therefore divided into three types. First were the electronic-content-related searches (all except powering the device on and dismantling it). Second were the low-severity traditional searches (the customs form, asking where the person had traveled, the simple drug-dog sniff search, opening the bag but not reading its contents, and the pat-down). Third were the remaining traditional searches. This division between high- and low-severity traditional searches was somewhat arbitrary; factor analysis did not yield clear and consistent groupings. But, based on the scores reported in Table 1, it seemed highly sensible to differentiate between searches that are routine and seen as generally low in intrusiveness and those that are not. The division was created based on whether more than 50 percent of the respondents believed that the search could be conducted on any traveler.[207]

Correlations were then conducted to examine the relationships between each of the search composite variables and each of the personality and demographic variables. Results are shown in Table 3. Several interesting patterns emerged. Most notably, the Westin privacy composite, which facially appears to tap information-privacy concerns, correlated with each of the three electronic-search composites such that those higher in privacy concern saw the searches as more intrusive, more embarrassing, and more likely to reveal sensitive information. The Westin composite does not correlate with views toward the low-severity searches and has a less consistent relationship with views toward the high-severity searches. Interestingly, neither political orientation, nor education, nor age correlated with the electronic-search attitudes.

In fact, political orientation does not appear to have any consistent relationship with search attitudes generally. Very few of the correlations are significant and, ignoring significance levels, about half the correlations are negative and about half are positive. The only significant effect is that the more socially conservative a

---

[207] The lowest value in the high-severity category was 68 percent and the highest in the low-severity category was 38 percent.

person is, the more he or she feels that high- and low-severity searches reveal sensitive information.[208] This is somewhat surprising given that there is a very slight negative correlation ($r(285) = -.12$, $p = .04$) between Westin's privacy composite and social conservatism.

[208] Note that all three measures used response scales ranging from "Very Liberal" to "Very Conservative." The items are termed "conservatism" only because higher values indicated greater conservatism and lower values greater liberalism.

TABLE 3. CORRELATIONS BETWEEN SEARCH ATTITUDES BY CATEGORY AND DEMOGRAPHIC CHARACTERISTICS

Search Category	Reliability	Westin Privacy	Education Level	Economic Conservatism	Social Conservatism	Conservatism	Age
Electronic Intrusiveness	.95	.166**	-.085	-.071	-.110	-.080	.101
Electronic Reveal Info	.95	.226***	-.075	.082	.067	.076	-.080
Electronic Embarrass	.95	.186**	-.107	-.046	-.045	-.058	-.042
Low-Severity Intrusiveness	.74	.091	-.088	-.084	.047	-.019	-.106
Low-Severity Reveal Info	.78	.008	-.100	.026	.171**	.101	-.119*
Low-Severity Embarrass	.77	.070	-.116*	-.038	.113	.039	-.098
High-Severity Intrusiveness	.75	.173**	-.010	-.061	-.050	-.058	.072
High-Severity Reveal Info	.80	.098	-.022	.013	.151*	.094	-.033
High-Severity Embarrass	.80	.124*	-.145*	-.039	.045	.002	.010

* $p < .05$; ** $p < .01$; *** $p < .001$

It was also possible to examine whether the degree to which people felt that their electronic devices could reveal different types of information about them affected their attitudes toward electronic searches. Correlations were conducted between the three electronic-search composites and the degree-of-exposure questions. Some categories of information were surprisingly unrelated to search attitudes, including banking information, prescriptions, educational records, and credit reports. Romantic interests, information about family and friends, ideology, and pornography interests, on the other hand, were the most consistently related to search attitudes, particularly expected embarrassment. In fact, seven of the eleven information domains correlated significantly with embarrassment ratings, but only four with revealing sensitive information and two with electronic intrusiveness.

TABLE 4. ATTITUDES TOWARD ELECTRONIC SEARCHES AS A FUNCTION OF THE EXTENT TO WHICH DIFFERENT TYPES OF INFORMATION WERE ON THE PARTICIPANT'S OWN ELECTRONIC DEVICES

Learn More From	Electronic Intrusiveness	Electronic Reveal Info	Electronic Embarrass
Banking Records	.053	.038	.088
Prescription Records	.044	.041	.096
Medical Info	.102	.060	.145*
Romantic Life	.136*	.127*	.186**
Educational Records	.035	.046	.100
Credit Records	.019	.013	.007
Recent Purchases	.113	.079	.159**
Income	.068	.063	.170**
Pornography Interests	.103	.120*	.159**
Ideology	.042	.128*	.206***
Info on Family and Friends	.137*	.148*	.208***

* $p < .05$; ** $p < .01$; *** $p < .001$

4. Differences among types of participants.

Particularly given that the sample was not perfectly representative of the population, it is important to consider the ways in which participant characteristics could have impacted search

attitudes. As shown in Table 3, participant age and political ideology had little bearing on search attitudes generally and no relation to attitudes toward electronic searches. A series of ANOVAs were used to test whether various dichotomous demographic characteristics had any effect on the nine search-attitude composites. Sex had no significant effects on any of the nine composites. Whether the participants currently held a valid passport or had traveled outside the country in the past year also had no significant effect on any composite. Whether the person had traveled outside the United States in the last five years produced a single significant difference: participants who had done so felt that the high-severity searches were marginally less likely to reveal sensitive personal information ($M = 57.63$, $SD = 19.75$) than those who had not ($M = 62.62$, $SD = 20.30$) ($F(1, 282) = 4.09$, $p = .04$, $\eta^2 = .014$).

Whether the person had traveled outside the United States *at any point* did affect views of some search types. As shown in Table 5, those who had traveled internationally thought that the low-severity searches—the types of searches that travelers are routinely subjected to—were less intrusive, less embarrassing, and less likely to reveal sensitive information. They also felt that high-severity searches were less embarrassing and less likely to reveal sensitive information, but to a much lesser extent (note the effect sizes). There were no differences on the electronic searches or on the perceived intrusiveness of high-severity searches.

TABLE 5. DIFFERENCES BASED ON EXTENT OF PRIOR TRAVEL EXPERIENCE

Search Category	Had the participant ever traveled outside the United States? Yes	No	$F(1, 281)$	η^2
Electronic Intrusiveness	89.37 (13.09)	90.40 (13.92)	0.34	.001
Electronic Reveal Info	80.31 (20.18)	83.71 (21.16)	1.57	.006
Electronic Embarrass	74.08 (23.06)	77.24 (23.56)	1.05	.004
Low-Severity Intrusiveness	37.58 (19.14)	45.66 (23.19)	8.98**	.031
Low-Severity Reveal Info	32.47 (19.98)	44.63 (24.00)	18.77***	.063
Low-Severity Embarrass	30.72 (20.56)	39.87 (23.44)	10.40**	.036
High-Severity Intrusiveness	78.26 (13.34)	79.36 (17.19)	0.32	.001
High-Severity Reveal Info	58.58 (19.32)	65.40 (21.05)	6.73**	.023
High-Severity Embarrass	67.46 (17.12)	72.31 (19.91)	4.18*	.015

* $p < .05$; ** $p < .01$; *** $p < .001$

It could be that travelers have become hardened to the low-severity searches from frequent exposure. In contrast, travelers almost never experience the electronic searches,[209] so those who have been abroad have not become more accustomed to them. This explanation is reminiscent of the circularity critique of reasonable expectations of privacy: it is reasonable to expect that which the government does often and reasonable to expect to be

[209] From October 2009 through April 2010, 168.2 million travelers entered the United States. Of these, 3.7 million (2.2 percent) were referred for secondary inspection, during which they were questioned and searched at greater length. Of these, 2,272 were subjected to inspection of electronic devices, or approximately 325 per month out of approximately 530,000 travelers. See Corbett, 81 Miss L J at 1299–1300 (cited in note 159).

free from that which the government does rarely.[210] The Supreme Court has stated, however, that holding a subjective expectation of privacy invasion need not remove Fourth Amendment protection. When an individual's subjective expectations are conditioned by "influences alien to well-recognized Fourth Amendment freedoms," a normative inquiry is proper.[211] For example, the Court might still recognize some Fourth Amendment protection were the government to announce a broad program of electronic searches, removing the subjective expectation of privacy.

On the whole, however, it appears that participants' views of border searches do not differ substantially based on their personality and demographic characteristics. No differences were observed for sex, having a valid passport, or having traveled in the preceding year, and only weak and inconsistent differences were observed for age and political ideology. Taken together with the correlation data in Table 3, this suggests that concern about the intrusiveness of searches at the border is not being driven by a particular group or category. People may have predicted that young people or liberals, for example, would be much more concerned about border searches. That does not appear to be the case in this sample.

IV. APPLYING THE RESULTS TO POLICY

The Fourth Amendment protects the privacy expectations "that society is prepared to recognize as 'reasonable.'"[212] The meaning of this reasonableness requirement has never been entirely clear.[213] Some scholars, such as Professor Slobogin, have treated the actual feelings and expectations of ordinary citizens as absolutely crucial, believing that the magnitude of the state's interest in performing a search should be weighed directly against the people's assessment of the search's intrusiveness.[214] Other scholars have proposed a more limited role for public opinion. Professor Kerr, for example, believes that Fourth Amendment

---

[210] See Kerr, 107 Mich L Rev at 958 (cited in note 190) (discussing the meaning of intrusiveness).

[211] *Smith v Maryland*, 442 US 735, 740 n 5 (1979).

[212] *Katz v United States*, 389 US 347, 361 (1967) (Harlan concurring). See also *Smith v Maryland*, 442 US 735, 739–40 (1979) (observing that Justice Harlan's concurrence in *Katz* offers the prevailing test for the application of the Fourth Amendment).

[213] See Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan L Rev 503, 504–05 (2007) (noting that the *Katz* test "remains remarkably opaque").

[214] See Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* 32–33 (Chicago 2007).

decisions can be best understood as combining four different models of reasonableness, each of which has been employed by the Court on different occasions.[215] Two of these models turn on public expectations. The probabilistic model asks whether a sensible person would expect to have his or her privacy protected in a given circumstance,[216] and the private-facts model asks whether the search is likely to reveal information that is "particularly private."[217] The other two models do not turn on public expectations: one asks whether the search requires a violation of positive law and the other whether the search is favored or disfavored on policy grounds.[218]

But even judges and policymakers adhering to Kerr's more restricted view of the role of public attitudes should be concerned about these data. The (presumably sensible) participants in this study reported that they believed that their electronic devices were free from searches absent at least reasonable suspicion. They also reported that searches of their laptops would reveal a great deal of personal and embarrassing information, more than would other searches. The probabilistic and private-facts models would therefore both support the conclusion that electronic searches should be restricted. Though these data are not the end of the analysis for Kerr (or even for Slobogin, who would weigh the state's interest), they should have some role in the reasonableness evaluation.

The present data also bear directly on the factors that the Court has held are relevant to the reasonableness of a border search. In *Flores-Montano*, the Court stated that highly intrusive searches of the person require some level of suspicion because they implicate the dignity and privacy interests of the person being searched.[219] Based on *Montoya de Hernandez*, the archetypal highly intrusive searches of the person are strip searches and body cavity searches.[220] The data reported here show that searches of electronic devices invoke privacy and dignity concerns to the same extent as body cavity and strip searches.[221] Specifically, electronic-device searches are more revealing of sensitive personal information and almost as embarrassing.

---

215 See Kerr, 60 Stan L Rev at 505–06 (cited in note 213).

216 Id at 508.

217 Id at 512.

218 See id at 522–23.

219 *Flores-Montano*, 541 US at 152.

220 See *Montoya de Hernandez*, 473 US at 541 n 4.

221 See Part III.D.1.

Therefore, if body cavity and strip searches at the border require reasonable suspicion because of the privacy and dignity concerns that they raise, so too should searches of electronic devices.

The data also show that people believe that their devices reveal a great deal about their lives. One pro-privacy commentator argues that "a laptop search could reveal just as much private information about a person as a strip search or other intrusive body search can, albeit of a different kind."[222] These data suggest that she understated the concern; people believe that *more* information is revealed from a laptop search than a strip search. If one conceives of intrusiveness in terms of privacy violation, then electronic searches are not merely among the most troubling, they *are* the most troubling.

This focus on information revelation helps show what is new about searches of electronic devices. Previous cases, such as *Flores-Montano*, have talked about the physical disruptiveness of searches because, in those cases, the objects seized were physical. Here the concern is information privacy, which raises a completely different set of issues.[223] If a physical object is handled and then returned promptly and intact, little harm has been done. If privacy has been "handled," it cannot be returned.

Since substantial privacy interests are implicated in searches of electronic devices, it is worth reconsidering the purposes underlying the government's countervailing interest in extensive border searches. The doctrine was created to control "who and what may enter the country."[224] Information does not generally cross the border at a checkpoint, nor does it fly into O'Hare and go through customs. Some commentators have argued that the border search exception should be seen as one of the many types of special-needs searches and, like the *Terry* stop, should be limited to its intended purpose.[225] A *Terry* stop is intended to protect police officers and the public at large from imminent threats, and its scope is limited to that aim.[226] An officer conducting

---

222 Alzahabi, Note, 41 Ind L Rev at 179 (cited in note 6).

223 See id at 178–79.

224 *Ramsey*, 431 US at 620.

225 See, for example, Alzahabi, Note, 41 Ind L Rev at 176 (cited in note 6); Sid Nadkarni, Comment, *"Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices*, 61 UCLA L Rev 148, 166–67 (2013); Ari B. Fontecchio, Note, *Suspicionless Laptop Searches under the Border Search Doctrine: The Fourth Amendment Exception That Swallows Your Laptop*, 31 Cardozo L Rev 231, 239–44 (2009).

226 See *Terry*, 392 US at 26.

a *Terry* stop can pat a person down for weapons but cannot probe for other contraband.[227] Perhaps the scope of border searches should be limited to keeping out illegal aliens and contraband, rather than extending to the pursuit of unrelated criminal investigations. This would remove the need for most searches of electronic devices.

With this in mind, it is worth considering the case of David House. House was a supporter of Chelsea (formerly Bradley) Manning, who leaked classified documents to Wikileaks.[228] Based on his activism, House was flagged to be searched at the border when he next left and reentered the country.[229] As a result, he was intercepted upon returning from Mexico and his computer was extensively searched.[230] In part because of ACLU intervention, House was able to pursue his claim against the government and ultimately reached a settlement giving him both access to documents describing how he had been targeted and an agreement that the seized data be destroyed.[231]

House's case shows the danger of allowing the government to use border crossings as an excuse to conduct searches unrelated to border security. The purpose of the border search exception is not to provide a pretext to circumvent the usual requirement of the Fourth Amendment. The exception exists to protect the nation from those threats that are uniquely present at border crossings. These are, as *Ramsey* reminds us, the exclusion of physical contraband and undesired persons.[232] Neither purpose requires, or is even meaningfully facilitated by, electronic-device searches.

CONCLUSION

The Fourth Amendment analysis weighs the privacy and dignity interests of the person being searched against the

---

227 Id at 27.

228 See *House v Napolitano*, 2012 WL 1038816, *2 (D Mass).

229 Id.

230 Id at *3.

231 See Ryan Gallagher, *Government Settles with Researcher Put on Watch List for Supporting Bradley Manning*, Slate Future Tense Blog (Slate May 30, 2013), online at http://www.slate.com/blogs/future_tense/2013/05/30/david_house_researcher_put_on_watch_list_for_supporting_bradley_manning.html (visited Aug 12, 2014). House's claim that his targeting was in response to his political activities and violated his First Amendment right to free association survived a motion to dismiss. See *House*, 2012 WL 1038816 at *10–13. For the settlement agreement, see https://www.aclu.org/files/assets/house_settlement.pdf (visited Aug 12, 2014).

232 See *Ramsey*, 431 US at 620.

government's need to conduct the search. The government's need is presumed to be quite strong at the border, so the balance generally tilts in its favor. But theories of the Fourth Amendment generally require some consideration of public attitudes. The data presented here demonstrate that the privacy and dignity interests implicated in searches of electronic devices are very powerful. They are more powerful, in fact, than some courts have presumed. Though these interests need not be decisive, they must be weighed.

Imposing a reasonable suspicion standard for searches of electronic devices would be a fairly modest step given the strength of the privacy interests implicated. Electronic-device searches are seen as among the most intrusive of those described in the current case law. They are *the* most revealing of sensitive information. They are only less embarrassing than strip searches and body cavity searches. And, finally, most people believe that such searches require not only reasonable suspicion, but also a warrant from a judge. The privacy interests at stake in these searches are therefore very strong.

When the Framers wrote the Fourth Amendment and later carved out an exception for border searches, they did not foresee the smartphone, the laptop, sexting, or cloud storage. But it is still worth recalling that the nineteenth century gave us cases like *Boyd v United States*,[233] which provided extensive protection to one's personal papers.[234] Given such historic concern for the privacy of correspondence and the avoidance of self-incriminating disclosures of documents, we should take seriously the public's current resistance to these searches. Particularly, we should give further thought to the extent and nature of the government's interests. Is the government's need for electronic searches at the border great enough to outweigh the dignity and privacy interests that we now know are implicated?

---

[233] 116 US 616 (1886).

[234] See id at 631–32 (stating that compelling the production of private papers "cannot abide the pure atmosphere of political liberty and personal freedom").