2014

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

Matthew B. Kugler

CHICAGO

COASE-SANDOR INSTITUTE FOR LAW AND ECONOMICS WORKING PAPER NO. 677
(2D SERIES)

COASE-SANDOR INSTITUTE
FOR LAW AND ECONOMICS
THE UNIVERSITY OF CHICAGO LAW SCHOOL

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

Matthew B. Kugler

THE LAW SCHOOL
THE UNIVERSITY OF CHICAGO

February 2014

The Perceived Intrusiveness of Searching Electronic Devices at the Border:

An Empirical Study

Matthew B. Kugler[1]

This paper presents new empirical data that seeks to quantify the privacy interests and expectations of regular people in the context of a border crossing. Courts have previously disagreed about whether travelers understand that their electronic devices are subject to search at the border, and whether such searches are more intrusive than routine examinations of traveler luggage. The data presented here show that, consistent with the view the 9th Circuit recently adopted in its controversial Cotterman decision, ordinary people believe that searches of their electronic devices impinge more on their privacy and dignity interests than do most traditional searches. In fact, survey participants tended to rate electronic searches as being almost as intrusive as strip and body cavity searches. In addition, the overwhelming majority of participants believed that their electronic devices could not be searched at a border crossing unless the customs agent had some level of individualized suspicion, suggesting that current doctrine creates substantial risk of surprise. These data will hopefully serve to shed light on the new issues raised by searches of electronic devices in an era of smartphones, tablets, and cloud computing.

Forthcoming, The University of Chicago Law Review.

[1] BA 2005, Williams College; PhD in Social Psychology 2010, Princeton University; JD Candidate 2015, The University of Chicago Law School.

INTRODUCTION

"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, 541 U.S. 149, 153 (2004).

"It is frightening the number of ways I had not even considered being 'violated' prior to this survey." Subject 189, after rating the intrusiveness of various border searches.

The Fourth Amendment protects the right of people to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[2] 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 – smart phones, 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; Fourth Amendment protections are substantially relaxed at the border. But, given the sheer amount of personal information that can be recovered from a smartphone's text message log or a computer's email archive, is it "reasonable" to give government agents unfettered discretion to search them?

Recently there has been much academic discussion – and some conflicting case law – on whether there should be restraints on searches of electronic devices at the border. Specifically, it has been proposed that such searches should require an elevated level of suspicion.[3] Those advocating for an elevated suspicion standard base their arguments on the role electronic devices now play in people's daily lives, the degree of intrusion into the privacy of individuals represented by an electronic device search, and the potential for surprise.[4] Courts have recognized the importance of these factors, particularly surprise. In Cotterman, 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."[5] Other courts have disputed that travelers will find searches of electronic devices any more intrusive or surprising than searches of their other possessions.[6]

I conducted an empirical survey study of approximately three-hundred adult Americans to measure the perceived intrusiveness of electronic device searches and the actual expectations of ordinary citizens. The results show that people see electronic device searches as comparable to strip searches and body cavity searches. Electronic searches are seen as the most revealing of sensitive

---

[2] US Const Amend IV.

[3] See, for example, United States v Ickes, 393 F3d 501, 505 (4th Cir 2005); United States v Cotterman, 709 F3d 952, 960 (9th Cir 2013).

[4] See generally John W. Nelson, Border Confidential: Why Searches of Laptop Computers at the Border Should Require Reasonable Suspicion, 31 Am J Trial Advoc 137 (2007); Rasha Alzahabi, Should you leave your laptop at home when traveling abroad?: The Fourth Amendment and Border Searches of Laptop Computers, 41 Ind L R 161 (2008).

[5] Cotterman, 709 F3d at 967.

[6] Ickes, 393 F3d at 502-06.

information, and are only slightly less embarrassing than the most intimate searches of the body. These searches, therefore, implicate the types of privacy and dignity concerns that the Court has stated may lead to an elevated suspicion requirement.[7] Also, most people believe that their electronic devices are not subject to search without cause at a border crossing, with many believing that a warrant is required. Just as the Ninth Circuit feared in Cotterman, there is substantial chance of unfair surprise.[8] By presenting the actual views and expectations of ordinary Americans, these data help quantify the civil rights concern that is being weighed against the government's interest in securing the border.

These data may also be relevant to a closely related issue in Fourth Amendment law. The Supreme Court recently granted certiorari in two cases involving searches of cell phones incident to arrest.[9] There, as in the border search context, the central claim of privacy proponents is that electronic devices are different than the address books, grocery lists, and briefcases that current doctrines were designed to handle.[10] Though there are many issues relevant to searches incident to arrest that are beyond the scope of this paper, the data discussed here do provide support for that key point: searches of sophisticated electronic devices are almost unique in their intrusiveness.

In Part I, I review 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 to the novel issues presented by searches of electronic devices. Part III presents the results of the above-mentioned 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, I will review the general case law on border searches. I 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 come in and search your house.[11] 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.[12] Border searches have historically been viewed as another exception to this 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

---

[7] See text accompanying notes 52-66.

[8] Id.

[9] United States v Wurie, 728 F.3d 1 (1st Cir. 2013) cert granted, 13-212, 2013 WL 4402108 (U.S. Jan. 17, 2014) (lower court prohibiting a cellphone search); People v Riley, D059840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013), cert granted in part, 13-132, 2013 WL 3938997 (U.S. Jan. 17, 2014) (lower court permitting a cellphone search).

[10] 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).

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

[12] 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).

effects is at its zenith at the international border."[13] Non-routine, more invasive, searches may require a showing of a low level of individualized suspicion, called "reasonable suspicion."[14]

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 customs 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.[15] The act specifically 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 place, store, building, or other place," for which the agents needed to seek a warrant.[16] Therefore searches at the border could be done at the discretion of the customs agents whereas searches by customs agents for smuggled goods at non-border 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. The Supreme Court has repeatedly stated that the border search exception's long history substantially strengthens the case for its constitutionality.[17]

The main wave of recent border search cases has concerned the smuggling of controlled substances. In the prohibition era case Carroll v United States,[18] the Court used the border search doctrine as a point of comparison as it devised a new exception to the warrant requirement for the search of automobiles.[19] The Carroll Court said "[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."[20] Automobile searches, in contrast, were held to require probable cause (though not a warrant) because the state did not have the same set of strong interests in the interior that it did at the border, where a search was presumptively reasonable even without probable cause.

The Court echoed the Carroll logic nearly 50 years later in United States v Ramsey,[21] stating that the sovereign has a strong interest in controlling "who and what may enter the country."[22] The case concerned the discovery of illegal drugs in a package mailed to the United States from Thailand.[23] By statute, postal inspectors had the power to open packages and inspect their contents without a warrant if they had "reasonable cause to suspect" the package contained contraband.[24] In holding

---

[13] United States v Flores-Montano, 541 US 149, 152.
[14] United States v Montoya de Hernandez, 473 US 531, 541 (1985).
[15] Act of July 31, 1789, Sec 24.
[16] Id.
[17] United States v Ramsey, 431 US 606, 616–17 (1977) (noting that the First Congress also passed the Bill of Rights, and that it therefore can be presumed to have not 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.").
[18] Carroll v United States, 267 US 132 (1925).
[19] The case concerned the smuggling of alcohol during prohibition.
[20] Carroll, 267 US at 132, 153–54.
[21] Ramsey, 431 US at 606.
[22] Id at 620.
[23] Id at 609.
[24] Id at 611.

the statute constitutional, the Court stated "that 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."[25]

The defendant in Ramsey attempted to raise a First Amendment challenge to the mail inspection because his "papers" were subject to search. However, the governing statute barred postal inspectors from reading any letters that were inside the packages they inspected.[26] Thus the "papers" contained in the mail were accorded greater security than the goods. Because reading the mail was prohibited, the Court explicitly did not reach the First Amendment issue.[27]

B. Requirement of Reasonable Suspicion for Non-Routine Searches

As suggested by the statutory limitation on reading correspondence in Ramsey, not all border searches are alike. Some searches, those considered non-routine, are only permissible if the border agent has reasonable suspicion.

The term "reasonable suspicion" has its origin in the Terry investigative stop cases.[28] It is defined as "a particularized and objective basis for suspecting the particular person stopped of criminal activity."[29] 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."[30] Reasonable suspicion cannot generally be found based purely on demographic characteristics, but it can be found if the suspect fits a detailed offender profile.[31]

Two Supreme Court cases help to define the category of non-routine searches, those that impose a reasonable suspicion requirement. In United States v Montoya de Hernandez,[32] the Court considered a particularly intrusive search. The defendant entered the United States at the Los Angeles International Airport having come from Bogota, Columbia. Upon arrival, she aroused suspicion based on inconsistencies and implausibilities in her story.[33] Based on his past experience, the customs inspector came to believe that Montoya de Hernandez was likely to be an alimentary canal smuggler.[34] She was offered the choice to leave the country, submit to an x-ray, or produce a monitored bowel movement. Ultimately, logistical problems prevented her from being able to take the first option, and she was detained for approximately 16 hours before the customs officials sought a warrant for an x-ray. The warrant was granted 8 hours later but, before the x-ray could take place, the defendant involuntarily produced a bowel movement that contained the first of many cocaine-filled balloons.[35]

---

[25] Ramsey, 421 US at 616.
[26] Id at 623.
[27] Id at 624.
[28] Terry v Ohio, 392 US 1 (1968).
[29] United States v Cortez, 449 US 411, 417–18 (1981).
[30] Terry, 392 US at 27.
[31] United States v Sokolow, 490 US 1, 10 (1989).
[32] 473 US 531 (1985).
[33] Montoya de Hernandez, 473 US at 533.
[34] Id at 534.
[35] Id at 534–36.

The question before the Court was whether the detention (which at minimum had to be measured as 16 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.[36] Because a warrant was obtained before a medical examination was ordered,[37] the Court specifically did not consider what level of scrutiny, if any, would be needed for a body cavity or strip search.[38] Given that reasonable suspicion was required for the detention, however, it would be somewhat difficult to imagine that a lower standard would be appropriate. Courts considering the question after Montoya de Hernandez have generally held that reasonable suspicion is required for strip searches at the border.[39]

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 the governmental interests.[40] 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."[41] At the border, the test is "qualitatively different" in that the balancing of interests is struck "much more favorably to the Government."[42] This is why routine border searches are not subject to any requirement of reasonable suspicion or probable cause.[43] In the Court's words, the border search cases "reflect longstanding concern for the protection of the integrity of the border." And "[t]his concern is, if anything, heightened by the veritable national crisis in law enforcement caused by smuggling of illicit narcotics."[44] For these reasons, the detention was permissible if reasonable suspicion was present.

Justices Brennan and Marshall filed a vigorous dissent in Montoya de Hernandez. Their main concern was the humiliating and degrading treatment Hernandez suffered during her detention.[45] They were worried that the reasonable suspicion standard gave "sweeping and unmonitored authority" to low-level customs officials.[46] But they were also interested in tethering the border search exception to its purpose. Though they believed that wide-ranging detentions and searches for immigration and customs control were "unquestioned," they also thought that "far different considerations apply when detentions and searches are carried out for purposes of investigating suspected criminal activity."[47]

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. In Arizona v Gant,[48] the Court held that a vehicle search incident to arrest was only proper to the extent it protected officer safety or was

---

[36] Id at 541.
[37] Id at 534–36.
[38] Montoya de Hernandez, 473 US at 541.**[ED: this should be "id," please change. NHJ]**
[39] See, for example, Tabbaa v Chertoff, 509 F3d 89, 98 (2d Cir 2007); United States v Johnson, 991 F2d 1287, 1292 (7th Cir 1993); United States v Ramos-Saenz, 36 F3d 59, 61 (9th Cir 1994).
[40] Id at 537.
[41] New Jersey v T.L.O., 469 US 325, 337–42 (1985).
[42] Montoya de Hernandez, 473 US at 538–40.
[43] Id.
[44] Id.
[45] Montoya de Hernandez, 473 US at 545–48 (Brennan, dissenting).
[46] Id at 549.
[47] Montoya de Hernandez, 473 US at 554 (1985) (Brennan, dissenting) (internal citations omitted).
[48] Arizona v Gant, 556 US 332 (2009)

likely to turn up "evidence relevant to the crime of arrest."[49] 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.[50] Brennan and Marshall 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."[51]

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

Montoya de Hernandez established that certain types of non-routine searches, such as detentions for 16 hours and potentially body cavity and strip searches, require reasonable suspicion. The boundaries of the category of non-routine searches were very unclear, however. The more recent case of Flores-Montano helps to distinguish this set of non-routine searches.[52] 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.[53] 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 reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person – dignity and privacy interests of the person being searched – simply do not carry over to vehicles."[54] In effect, the Court held that non-routine searches were those that were highly intrusive to the dignity and privacy interests of those being searched, and not those that were merely unusual or required 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."[55] 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 recognition of this.[56] No private, intimate activity occurs in a car's gas tank, and no legitimate secrets are commonly stored there.

The innocent also have nothing to fear from a gas tank search. As the Court noted, a gas tank should be solely a repository for fuel.[57] No great embarrassment or personal revelations are risked by allowing it to be subject to search. Indeed in my empirical survey, participants rated gas tank searches as among the least revealing of sensitive personal information.[58] As Justice Stevens noted in Montoya de Hernandez, to allow a search without reasonable suspicion is to accept that a greater

---

[49] Id at 343-44.
[50] Indianapolis v Edmond, 531 US 32, 37 (2000).
[51] 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 Brennan and Marshall recognize as legitimate.
[52] Flores-Montano, 541 US at 149.
[53] Id at 151–52.
[54] Id at 152.
[55] Id at 154.
[56] See generally California v Acevedo, 500 US 565 (1991) (describing the vehicle search exception).
[57] Flores-Montano, 541 US at 154.
[58] See text accompanying notes 151–154.

share of innocent people will be subjected to it.[59] Here, those innocent people would suffer inconvenience, but 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.[60] The gas tank search here, however, did not satisfy either requirement.[61]

The question in the wake of Flores-Montano is whether the "dignity and privacy interests of the person being searched"[62] ever require limitations on searches of property. 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.[63] Lower court judges trying to apply Flores-Montano to searches of electronic devices have differed on this point.[64]

II. Border Searches and Electronic Devices

Electronic devices pose novel challenges to 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.[65]

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?), their laptops and cellphones contain many: office gossip, prescriptions for anti-depressants, 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. Do searches of mobile electronic devices then 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, the Ninth Circuit has instead viewed them as sui generis, imposing a reasonable suspicion requirement for some searches.[66] In reaching these conflicting results, the circuits have disagreed about the expectations of travelers at the border[67] and whether the privacy and dignity interests described in Flores-Montano are implicated by laptop searches.[68]

---

[59] Montoya de Hernandez, 473 US at 545 (Stevens concurring) (stating that even a requirement of reasonable suspicion will still allow for the searches of many innocent people).
[60] Flores-Montano, 541 US at 155–56.
[61] Id.
[62] Id at 152.
[63] Id.
[64] See notes 92-94 and accompanying text.
[65] Flores-Montano, 541 US at 155–56.
[66] Compare Ickes, 393 F3d at 502, with Cotterman, 709 F3d at 959.
[67] Compare Ickes, 393 F3d at 506, with Cotterman, 709 F3d at 967.
[68] Compare Ickes, 393 F3d at 505–6, with Cotterman, 709 F3d at 966.

A. The Fourth Circuit Approach: Electronic Devices as Unexceptional

In the first appellate case on this issue, United States v Ickes,[69] the Fourth Circuit did not require reasonable suspicion to justify the search of a computer at the Canadian border.[70] 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.[71] In holding that the search statute in question 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.[72] "Both Congress and the Supreme Court have made clear that extensive searches at the border are permitted, even if the same search elsewhere would not be. We refuse to undermine this well-settled law by restrictively reading [the statute]..."[73] The Ickes court also rejected the argument that there should be a First Amendment exception for expressive materials.[74]

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.'"[75] The court saw no reason why searches of electronic devices were less expected than any other type of search.

Though the court held that reasonable suspicion was not required, Judge 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."[76] He emphasized that customs officials simply do not have the resources to search every computer.[77] Because the mechanical cost of the search is high, there was arguably no need to also impose a legal barrier.

Perhaps important in the Ickes case is that there was no question 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."[78] This would normally amount to at least reasonable suspicion that child pornography would be present on Ickes's electronic devices. 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."[79] 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, nor even mere probable cause, but a freely given confession.

---

[69] Ickes, 393 F3d at 501.
[70] Id at 505.
[71] Id at 502.
[72] Id.
[73] Id at 502.
[74] Ickes, 393 F3d at 506–07.
[75] Id.
[76] Ickes, 393 F3d at 507.
[77] Id.
[78] Id at 503.
[79] Id.

It is sometimes said that easy cases make bad law. For the search of Ickes to be invalid, the Fourth Circuit would have needed to impose a warrant requirement for the searches of expressive materials, or to hold that electronic devices were not covered in the border search statute. Neither holding could easily be supported by past precedent.[80] The outcome of the Ickes case was therefore in little doubt. Because the case would not have come out differently had the law required some elevated level of suspicion, 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. These factors 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."[81] In ruling against him, Judge Wilkinson wrote "[t]his prediction seems far-fetched. Customs agents have neither the time nor the resources to search the contents of every computer."[82]

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.[83] 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, the agent began with a cursory examination of the 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."[84] Though the government did not argue that these pictures depicted minors,[85] Arnold was nevertheless detained for several hours as his laptop was searched. The agents eventually found child pornography.[86]

Though the Ninth Circuit would later adopt some measure of protection against laptop searches, in this case it followed the Fourth Circuit's example: holding that the search did not require reasonable suspicion.[87] Foreshadowing the questions it would address in Cotterman, 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."[88] Arnold had attempted to analogize laptops to homes, particularly

---

[80] Id at 504-5; Id at 507.
[81] Id at 506–07.
[82] Id.
[83] United States v Arnold, 533 F3d 1003 (9th Cir. 2008) (according to the district court opinion, the search was random, see note 86).
[84] Id at 1005.
[85] United States v Arnold, 454 F. Supp. 2d 999, 1001 (C.D. Cal. 2006) rev'd, 523 F3d 941 (9th Cir. 2008) opinion amended and superseded on denial of reh'g, 533 F3d 1003 (9th Cir. 2008).
[86] Arnold, 533 F3d 1003, 1005 (9th Cir. 2008)
[87] Id at 1006.
[88] Id.

citing the amount of personal documents likely to be stored on them and the amount of secrets that could be revealed by their search.[89] 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."[90] Though laptops contain substantial personal and expressive material, the court saw no reason to differentiate their search from any of the other searches 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."[91]

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. 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."[92] But neither exception applied here: the behavior of the customs agents appeared to have been professional and the laptop itself was undamaged.[93]

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, and that the privacy and dignity interests of the searched party were not implicated by allowing a search of that area. The same cannot be said of a laptop search. This alternative interpretation of Flores-Montano was at the core of the District Court's contrary ruling.[94]

C. The Ninth Circuit, Revisited

In a self-described "watershed case," the Ninth Circuit revisited the border search doctrine in United States v Cotterman.[95] Cotterman was entering the United States from Mexico. His identity was flagged based on a fifteen-year-old conviction for child molestation and, with relatively minimal additional cause, his laptop was searched.[96] The agents conducted a cursory examination of the laptop, as in Arnold, but initially found nothing. The laptop was then shipped almost 170 miles away and subjected to a comprehensive forensic examination. Only then were images of child pornography discovered.[97] Initial analysis found seventy-five images of child pornography within the unallocated space of Cotterman's laptop.[98] "In many of the images, Cotterman was sexually molesting the child."[99] The questions presented were whether the escalation from a cursory

---

[89] Id.
[90] Id at 1007.
[91] Arnold, 533 F3d at 1007 (internal citations omitted).
[92] Id at 1008–09.
[93] Id.
[94] United States v Arnold, 454 F. Supp. 2d 999, 1003 (C.D. Cal. 2006) rev'd, 523 F3d 941 (9th Cir. 2008) opinion amended and superseded on denial of reh'g, 533 F3d 1003 (9th Cir. 2008).
[95] 709 F3d 952, 956 (9th Cir. 2013)
[96] Cotterman, 709 F3d at 956.
[97] Id.
[98] Id at 958.
[99] Id at 959.

examination at the border to a forensic examination off-site should have required reasonable suspicion, and whether reasonable suspicion was present.[100]

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.'"[101] 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 in the manner in which they are carried out.[102] 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. 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."[103] 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."[104]

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."[105] As in Ickes,[106] the court here is making an empirical claim about what ordinary people expect, and assigning legal significance to its assumptions.

Despite adopting the defendant in Arnold's take on the importance of electronic devices, the Ninth Circuit did not overrule that decision. It held that the legitimacy of the initial search of Cotterman's laptop was not in doubt. Only the "comprehensive and intrusive" forensic examination that followed triggered a reasonable suspicion requirement.[107] This was due to the especially intrusive nature of 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."[108] Computer forensics is 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."[109] This was "essentially a computer strip

---

[100] Id at 957.
[101] Id at 960.
[102] Cotterman, 709 F3d at 963.
[103] Id at 964.
[104] Id. It is unclear why, if the listing of "papers" is of great importance, the listing of "effects" is not.
[105] Cotterman, 709 F3d at 967.
[106] Ickes, 393 F3d at 506–07.
[107] Cotterman, 709 F3d at 962.
[108] Id at 962–63.
[109] Id at 957.

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."[110]

This is very much an Entick and Wilkes type argument about the evils of giving officials wide discretion to search private papers (though those cases are not named).[111] The Fourth Amendment was created, in part, to prevent the state from having the power to conduct a general fishing expedition through a person's private papers and effects.[112] In the eyes of the majority, the extent of this "border search" was such that the privacy interests of the target were eviscerated.[113]

1. Adapting doctrine to account for changes in technology

The Cotterman court believed that existing border search doctrines needed to be updated to account for the effects of changes in technology.[114] As support for this type of doctrinal tailoring, the court cited Kyllo v United States,[115] which found that government monitoring of a home's heat signature is a search within the meaning of the Fourth Amendment. Prior to the development of thermal imaging devices, no one would have thought that monitoring waste heat would amount to a privacy violation. Given what technology had made possible by the beginning of the 21st century, however, such signals could be used to peer within the private protected space of the home. The majority in Cotterman believed that this presented a parallel case: the intrusion of a search of one's traveling possessions had previously been small but, with the rise of mobile computing, had increased substantially.[116]

First, the majority was concerned with the sheer magnitude of the amount of information carried.[117] Though a person might select a few files out of a cabinet to carry in a briefcase, the laptop amounts to the entire filing cabinet, if not the entire office. This contributes to the further problem that one does not select the files one carries on a laptop in the same way that one selects the papers one puts in a briefcase. This is particularly true in cases where deleted files are recovered; 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 cannot make meaningful decisions about what they are exposing to potential search.[118]

The type of information involved also presented a problem. The majority referred to "[l]aptop computers, iPads and the like" as being "simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails."[119] This is far beyond what would normally be found in a briefcase. As demonstrated in Table 2, below, participants in the survey study agree with the Ninth Circuit that more is exposed by their personal electronic devices than by their other luggage.

---

[110] Id at 966.
[111] See Akhil R. Amar, The Fourth Amendment, Boston, and the Writs of Assistance, 30 Suffolk U L Rev 53, 65–67 (describing how the Fourth Amendment was in part a response to the excesses of general warrants in the English cases of Entick and Wilkes).
[112] Id. See also James Otis, Against Writs of Assistance, 1761.
[113] Cotterman, 709 F3d at 957.
[114] Id at 956-57.
[115] 533 US 27 (2001).
[116] Cotterman, 709 F3d at 965.
[117] Id at 964.
[118] Id at 965.
[119] Id at 964.

Though it was not at issue in this case, the Cotterman court also commented on a problem that often arises in cellphone 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 likened using a mobile electronic device as "akin to a key to a safe deposit box."[120] 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, and Facebook, it may be possible to recover those passwords with a forensic examination. The potential for privacy intrusion is 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 they have merely tapped the mail icon on your phone, they have actually asked your phone to communicate with servers located in the US and, impersonating you, have downloaded data.[121] Customs agents searching smartphones apparently do regularly open apps,[122] so this is not a purely academic concern.

Because such a "thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity," the 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."[123]

2. The dissent, an endorsement of Ickes.

The Ninth Circuit's opinion drew a strong dissenting opinion from Judge Callahan. She concurred in the judgment – the majority found reasonable suspicion and held the evidence was admissible[124] – but sharply disagreed with requiring elevated suspicion for any search of an electronic device. She would have instead relied on the logic endorsed in Arnold: that reasonable suspicion should only be required for "(1) 'highly intrusive searches of the person'; (2) 'searches of property [that] are so destructive as to require' reasonable suspicion; and (3) searches carried out in a 'particularly offensive manner' (emphasis in original)."[125] In adopting this interpretation, she 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?

Callahan also attacked the majority's main premise that computers are intensely private. She pointed out that people regularly share intensely 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

---

[120] Id at 965.
[121] Id at 965.
[122] Patrick E. Corbett, The Future of the Fourth Amendment in a Digital Evidence Context: Where Would the Supreme Court Draw the Line at the International Border? 81 Miss LJ 1262, 1268 (2012) (describing the Abindor case).
[123] Id at 968.
[124] The dissent also pointed out that the majority had to make some fairly convoluted assumptions to find reasonable suspicion in this case. Cotterman, 709 F3d at 990–93 (Judge Callahan, concurring in part, dissenting in part, and concurring in the judgment). Again, it should be remembered that the class of defendants bringing these computer search cases consists of 1) child pornographers, and 2) child molesters.
[125] Id at 982.

elsewhere."[126] If Google searches are not private from Google, why should they be private from customs agents?

She also specifically rejected the argument that the quantity of data stored in electronic devices should change the analysis. "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."[127] 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."[128] Effectively, the majority was arguing that size mattered, and Judge Callahan saw no basis in the doctrine for that conclusion.[129]

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.[130] Some courts have explicitly held reasonable suspicion irrelevant to the more routine computer searches at issue in their particular facts.[131] Others have found reasonable suspicion and not determined whether it was necessary.[132]

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.[133] A more extensive and much-anticipated opinion in Abidor v Napolitano reached a similar result; holding that reasonable suspicion was present, making whether it was required moot.[134] That case concerned a challenge to the Department of Homeland Security directives that authorize the search of electronic devices at border crossings.[135] In reaching its conclusion, the court emphasized that travelers knew their electronic devices were at risk of both search and theft, and therefore would be wise to choose carefully what files they carried with them.[136]

---

[126] Id at 982; see also id at 986 (same dissent, noting that 500 million people are members of Facebook and that internet cookies are ubiquitous).
[127] Id at 965–66.
[128] Id at 987.
[129] Id.
[130] See Corbett, 81 Miss LJ at 1269–74 (cited in note 122). In his review of lower and appellate court decisions on border searches of electronic devices, Corbett finds 15 cases, 14 of which concern child pornography, over a 5 year period. The only appellate case described, apart from the Fourth and Ninth Circuit decisions, was United States v Irving, 452 F3d 110, 124 (2d Cir 2006). The court in that case did not decide whether a search of 3.5 inch computer discs was routine or non-routine because it was supported by reasonable suspicion.
[131] United States v Stewart, 729 F3d 517, 524 (6th Cir. 2013).
[132] United States v Rogozin, No 09-CR-379(S)(M), 2010 US Dist LEXIS 121162, at *9 (WDNY Nov 16, 2010); United States v Verma, No H-08-699-1, 2010 US Dist LEXIS 34559, at *12 (SD Tex Apr 8, 2010).
[133] United States v Wallace, 1:12-CR-230-1-TWT, 2013 WL 1702791 (ND Ga Apr 19, 2013).
[134] Abidor v Napolitano, 10-CV-04059 ERK JMA, 2013 WL 6912654 (E.D.N.Y. Dec. 31, 2013)
[135] Id.
[136] Id.

Perhaps the most important citation to Cotterman is a case outside the border search context. In the aforementioned cellphone search case of United States v Wurie,[137] the First Circuit favorably cited Cotterman as recognizing the need to tailor existing Fourth Amendment doctrine to deal with the realities of cellphones and other electronic devices.[138] As Wurie is now before the Supreme Court, the question of whether the Cotterman analysis is persuasive is of immediate importance.

III. An Empirical Study of Lay Attitudes and Expectations

As was 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. They have, in part, based their rulings on these impressions.[139] 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 needed to guess at the background social facts, even though these facts are highly relevant to their decisions. As was seen in the argument between the majority and dissent in Cotterman about the degree of security individuals have and expect in their electronic communications,[140] not all judges have arrived at the same set of answers. As judges and justices are now weighing whether the Cotterman court was correct 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 Christopher Slobogin and Joseph Schumacher. In the early 1990s, Slobogin and Schumacher conducted a survey asking a student sample to rate the perceived intrusiveness of a variety of types of searches drawn from controversial Fourth Amendment cases.[141] 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 phone for 30 days were seen as only slightly less intrusive.[142] 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.

This study was recently replicated by Jeremy Blumenthal, Meera Adya, and Jacqueline Mogle.[143] 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

---

[137] 728 F.3d 1 (1st Cir. 2013) cert granted, 13-212, 2013 WL 4402108 (U.S. Jan. 17, 2014).
[138] Id at 8.
[139] See notes 66 – 68 and accompanying text.
[140] Cotterman, 709 F3d at 986 (Judge Callahan, concurring in part, dissenting in part, and concurring in the judgment) (commenting that individuals regularly convey to Google the very sensitive personal information that is at issue in electronic searches).
[141] 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).
[142] Id at 738–39.
[143] 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 (2009).

bedroom were all more intrusive than the body cavity search.[144] The scenarios used in this study were the same as in Slobogin and Schumacher's, 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. Consider the personal diary example. Like the mobile electronic device, it can be searched without harm to it or physical contact with the person. But, again like the mobile device, searching it 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 student samples, and even the more recent of the studies is a decade old. Given the swiftly changing technological world, it is hard to know how people would feel after so much time has passed. The dependent measure was also somewhat limited. Slobogin and Schumacher had their participants rate "intrusiveness," and the replication study followed their example. Orin Kerr has argued that this is not the best term. He believes that the term "intrusive" "suggests interference with 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."[145] But merely because something is uncommon does not mean it violates civil liberties (and merely because it is common does not mean that it does not).[146] 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.[147] The resulting set of respondents was diverse, if not representatively weighted. 10 participants were excluded for having completion times that were less than half that of the median participant, and a further 5 were eliminated because they reported that they were not US citizens, leaving 285. Of the remaining sample, the median age was 35 (range 18-74, M = 37.56, SD = 12.77). 54.7% of the sample was female, 46.7% held a valid passport, and 72.1% had traveled outside the United States at some point. According to the State Department, in 2012 there were 113.4 million passports in circulation for 313.9 million Americans (35%),[148] making the sample more travel-ready than the national population as a whole. The sample was also somewhat better educated, with a

---

144 Id at 359.

145 Orin Kerr, Do We Need a New Fourth Amendment?, 107 Mich L Rev 951, 958 (2009).

146 Id at 959.

147 For a description of Mechanical Turk's use as a data collection tool, see Michael Buhrmester, Tracy Kwang, & Sam D. Gosling. Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? Perspectives on Psychological Science, 6, 3–5 (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 & Matthew B. Kugler, Public Perceptions of White Collar Crime Culpability: Bribery, Perjury, and Fraud, 75 L & Contemp Probs, 33, 42 (2012).

148 http://travel.state.gov/passport/ppi/stats/stats_890.html

greater number of participants holding four-year college degrees.[149] 85.6% of the sample was White, 6.7% was Black, and 5.3% was South or East Asian.

C. Types of Searches

Each participant was asked to evaluate twenty-six different types of search. 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 where they have been traveling and what they did there.
- 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.
- Search the traveler's car for any packages they might be carrying and open the packages.*[150]
- Have a drug-sniffing dog walk around the traveler's car.*
- Take the traveler's car to a location 90 minutes away and have a drug-sniffing dog walk around it.*
- Open the traveler's briefcase or backpack to check whether it contains drugs, but not to read any papers that might be inside.
- Open the traveler's briefcase or backpack and read any papers that might be inside.
- Fingerprint the traveler.
- Pat-down 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.
- Strip search the traveler.
- Perform a body cavity search on the traveler.

"The following questions concern the search of various electronic devices, such as cellphones, laptops, and tablets. [Following this preamble, the same prompt as above was used]"

- Power on the traveler's device.
- Dismantle the traveler's device to inspect the inside, assuming that it can be reassembled without damage.
- 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 entire text message history.

---

[149] In the sample 12.6% had graduate degrees, 36.8% had four year college degrees, 20.4% had two year degrees, 28.8% had high school degrees, and 1.4% had not completed high school. According to the US Census Bureau, 12.7% of those 35–39 have graduate degrees, a further 22.6% have four year degrees, 10.8% have two year degrees, 42.8% have a high school degree but have not completed any college degree, and 11.2% do not have a high school degree.
http://www.census.gov/hhes/socdemo/education/data/cps/2012/tables.html

[150] For those scenarios marked with a star, the text instead asked participants to picture only a land crossing.

- Search the traveler's entire picture archive.
- Search the traveler's device's browser for a list of recent searches.
- Review the traveler's most recently opened documents and applications.
- 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's saved passwords to log on to other websites, like Amazon or Ebay, to examine recent purchases.
- Use the traveler's device to read the traveler's electronic diary.
- Subject the traveler's device to a forensic examination to recover any files that the traveler may have deleted, including pictures, documents, and emails.

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 "[w]hether 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. The final question for each search asked participants whether the government could conduct this search on "any traveler they choose," "only if they can give a particular reason to suspect the specific traveler of criminal activity" (intended to capture the meaning of reasonable suspicion), or "only if they have a warrant from a judge."

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.[151] The results are presented in Table 1. The most severe of the electronic searches are seen as nearly as intrusive as the 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 the first mundane search other than those two body searches. Every electronic search that accessed the contents of the device was seen as significantly more intrusive than reading the papers in a traveler's briefcase, the analogy

[151] 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 scenario. 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.

drawn in the Cotterman dissent. All electronic searches, except merely turning the device on, were more intrusive than the search of the inside of a car's gas tank (which does not require reasonable suspicion under Flores-Montano). 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 90-minute drug dog inspection from United States v Place.[152] The single exception is turning the device on to see if it works.

The four searches seen as most revealing of private information are all of 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. Drawing a distinction that is somewhat supportive of a recent search incident to arrest case,[153] participants view the retrieval of recent call information as much less revealing than any of the other content-driven electronic searches.

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 that, however, is reading a person's personal diary and a range of electronic searches (the email account, the text archive, the deleted files, the picture archive), all of which are statistically and practically impossible to distinguish from each other. Here too, 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.[154] The judges in Cotterman were more correct than they likely believed. For the majority of electronic searches, including those that even the Cotterman court would have considered routine, less than 11% of participants believed that border agents could conduct the search without at least some articulable suspicion. For only 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% of participants still believed 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, 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

---

[152] United States v Place, 462 US 696 (1983) (holding that a 90 minute detention to allow for a drug dog sniff exceeded the permissible limits of a Terry stop).

[153] United States v Flores-Lopez, 670 F3d 803, 807–09 (7th Cir 2012) (Judge Posner arguing that cellphone searches incident to arrest might be subject to limitations, but that recovering the phone's own number or other minimal information is permissible).

[154] Cotterman, 709 F3d at 967; Ickes, 393 F3d at 506.

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% of respondents. In terms of the Flores-Montano dignity and privacy criteria, this would be a perverse result.

Table 1: Ratings of each search, with searches sorted by perceived intrusiveness.

N=285	Intrusiveness			Reveals Sensitive Information			Embarrassing			Expected Standard		
										Any Traveler	Reasonable Suspicion	Warrant
Traditional Searches												
Body Cavity	95.97	a	(12.36)	64.66	hi	(35.47)	96.44	a	(12.63)	9%	47%	43%
Strip Search	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 But Not Read Papers	50.07	mn	(29.33)	47.13	k	(31.84)	39.91	j	(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 where they have traveled and what they did there	26.89	o	(27.66)	27.70	n	(26.76)	17.48	l	(24.28)	88%	11%	1%
Electronic Searches												
Forensic Deleted Files	94.08	abc	(11.95)	89.01	a	(20.57)	81.72	b	(25.83)	8%	14%	78%
Email 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	abc	(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 Documents & 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	efg	(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%

Means are reported with standard deviations in parentheses. Means within a column that share a subscript are not significantly different from each other. For example, a search of a Facebook account (ef) is significantly more intrusive than a search of recent texts (g), but 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: your banking information; the prescriptions you have been on in the past; other sensitive medical information; information about your romantic interests or sex life; educational records; credit history; your recent purchases; your income level; your interests in pornography; your ideological beliefs; information about the personal lives of your friends and family. Participants then were asked to think about the other things they travel with and to rate whether someone searching their electronic devices would learn 1 ("no more than from my other possessions") to 5 ("much more than from my other possessions") about each information type from searching their electronic devices.

Table 2: Whether each type of information is present or absent on the person's own electronic devices, and the degree to which someone could learn more about the topic from their electronic devices than from their other travel possessions.

Type of information	Present	Absent	Learn How Much More from Electronic Search?			
Recent Purchases	82%	18%	3.58	(1.46)	t(284) = 29.87	***
Banking	76%	24%	3.41	(1.56)	t(284) = 26.09	***
Family Information	76%	24%	3.51	(1.41)	t(284) = 29.93	***
Romantic Life	55%	45%	2.89	(1.56)	t(283) = 20.49	***
Pornography	45%	55%	2.59	(1.71)	t(282) = 15.59	***
Credit	42%	58%	2.63	(1.58)	t(282) = 17.39	***
Income	41%	59%	2.60	(1.45)	t(283) = 18.52	***
Ideology	39%	61%	2.53	(1.46)	t(282) = 17.60	***
Educational Records	35%	65%	2.35	(1.48)	t(284) = 15.36	***
Medical	28%	72%	1.98	(1.35)	t(283) = 12.23	***
Prescriptions	23%	77%	1.93	(1.37)	t(284) = 11.43	***

The t-tests are for comparisons between each observed mean and the value 1 (no more than from my other possessions). * $p < .05$; ** $p < .01$; *** $p < .001$.

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 demographics information.[155] They also rated how liberal or conservative they are 1.) overall, 2.) on economic issues, and 3.) on social issues on scales ranging from 1 – Very liberal to 7 – Very conservative.

It is also interesting 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 Alan Westin.[156] Participants rated how much they agreed or disagreed with three statements on scales 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). [157] I averaged the items to create a composite ($\alpha = .72$) coded so that higher scores indicated greater privacy concern.

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 concern about email would be fundamentally different than the factors underlying privacy concern 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 search, and opening the bag but not reading the contents, 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 were routine and seen as generally low in intrusiveness and those that were not. The division was created based on whether more than 50% of the respondents believed that the search could be conducted on any traveler.[158]

Correlational analyses were then conducted examining 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

---

[155] See text accompanying notes 147—148 for the sample's distributions on these.

[156] For an overview of Westin's work, see Ponnurangam Kamaraguru and Lorrie Faith Cranor, Privacy Indexes: A Survey of Westin's Studies, Inst for Software Res Int'l, Carnegie Mellon University, Tech Rep, CMU–ISRI–5–138 (2005).

[157] Id at 13.

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

did 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. Interestingly, the only significant effects are such that the more socially conservative a person is, the more they feel that certain kinds of searches reveal sensitive information.[159] This is somewhat surprising given that there is a slight negative correlation $r(285) = -.12$, $p = .04$ between Westin's privacy composite and social conservatism.

Table 3: Correlations between search attitudes by category and demographic characteristics.

	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. Correlational analyses were conducted using the three electronic search composites as target variables and the degree of exposure questions as predictor variables. 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, 7 of the 11 information domains correlated significantly with embarrassment ratings, but only 4 with revealing sensitive information and 2 with electronic intrusiveness.

[159] 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 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	.053		.038		.088	
Prescriptions	.044		.041		.096	
Medical Information	.102		.060		.145	*
Romantic Life	.136	*	.127	*	.186	**
Educational Records	.035		.046		.100	
Credit	.019		.013		.007	
Recent Purchases	.113		.079		.159	**
Income	.068		.063		.170	**
Pornography Interests	.103		.120	*	.159	**
Ideology	.042		.128	*	.206	***
Family and Friends Info	.137	*	.148	*	.208	***

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

4. Differences among types of participants

Particularly given that the sample was not perfectly representative, it is important to consider the ways in which participant characteristics could have impacted search attitudes. As was shown in Table 3, participant age and political ideology had little bearing on search attitudes generally and no relation to attitudes toward electronic searches. Using a series of ANOVAs, I tested 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 US in the last five years produced a single significant difference: participants who had done so felt 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 or not the person had traveled outside the United States at any point did have some effect on views of some search types. As can be seen in Table 5, those who had traveled 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.

Had the participant ever traveled outside the US?						η^2
	Yes		No			
Electronic Intrusiveness	89.37	(13.09)	90.40	(13.92)	$F(1,281) = 0.34$	.006
Electronic Reveal Info	80.31	(20.18)	83.71	(21.16)	$F(1,281) = 1.57$	.004
Electronic Embarrass	74.08	(23.06)	77.24	(23.56)	$F(1,281) = 1.05$	.001
Low Severity Intrusiveness	37.58	(19.14)	45.66	(23.19)	$F(1,281) = 8.97$, $p = 0.003$	.031
Low Severity Reveal Info	32.47	(19.98)	44.63	(24.00)	$F(1,281) = 18.77$, $p < .001$	.063
Low Severity Embarrass	30.72	(20.56)	39.87	(23.44)	$F(1,281) = 10.40$, $p = 0.001$	.036
High Severity Intrusiveness	78.26	(13.34)	79.36	(17.19)	$F(1,281) = 0.32$	.001
High Severity Reveal Info	58.58	(19.32)	65.40	(21.05)	$F(1,281) = 6.73$, $p = 0.01$	.023
High Severity Embarrass	67.46	(17.12)	72.31	(19.91)	$F(1,281) = 4.18$, $p = 0.042$	.015

It could be that travelers have become hardened to the low severity searches from years of frequent exposure. In contrast, travelers almost never experience the electronic searches,[160] 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 free from that which the government does rarely.[161] The Supreme Court has stated, however, that 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.[162] Were the government to announce a broad program of electronic searches, removing the subjective expectation of privacy, the Court might still recognize some Fourth Amendment protection.

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 for age and political ideology.

IV. Application of results to policy.

The Fourth Amendment protects the privacy expectations "that society is prepared to recognize as 'reasonable.'"[163] The meaning of this reasonableness requirement has never been entirely clear.[164] Some scholars, for example Christopher 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

[160] From October 2009 through April 2010, 168.2 million travelers entered the United States. Of these, 3.7 million (2.2%) were referred for secondary inspection, where they were questioned and searched at greater length. Of these, 2,272 were subjected to inspection of electronic devices, approximately 325 per month out of approximately 530,000 travelers. See Corbett, 81 Miss LJ at 1299–1300 (cited in note 122).

[161] See also Kerr, 107 Mich L R at 958 (cited in note 145) (discussing the meaning of intrusiveness).

[162] Smith v Maryland, 442 US 735, 741 (1979)

[163] Katz v United States, 389 US 347, 361(1967) (Harlan, concurring).

[164] See generally Orin S. Kerr, Four Models of Fourth Amendment Protection, 60 Stan L Rev 503, 505 (2007)

intrusiveness.[165] Other scholars have circumscribed a more limited rule for public opinion. Orin Kerr, for example, believes that Fourth Amendment decisions can be best understood as combining four different models of reasonableness each of which has been employed by the Court on different occasions.[166] Two of these models turn on public expectations. The probabilistic model asks whether a sensible person would expect to have privacy protected in those circumstances,[167] and the private facts model asks whether the search is likely to reveal information that is "particularly private."[168] The other two models do not: one asks whether the search requires a violation of positive law and the other whether the search is favored or disfavored on policy grounds.[169]

Even judges and policymakers using 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 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 do other searches.. The probabilistic and private facts models would therefore both lead to the conclusion that electronic searches should not be unrestricted. Though these data are not the end of the analysis for Kerr (or even for Slobogin, who would weigh the state's interest), they do and should have some role in the reasonableness evaluation.

The present data 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.[170] Based on Montoya de Hernandez, the archetypal highly intrusive searches of the person are strip searches and body cavity searches.[171] The data reported here show that searches of electronic devices invoke privacy and dignity concerns to the same extent as do body cavity and strip searches.[172] Specifically, they are more revealing of sensitive personal information, and almost as embarrassing. Therefore, if body cavity and strip searches at the border require reasonable suspicion because of the privacy and dignity concerns 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 argued 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."[173] This data suggests 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.

---

[165] Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 32-33 (Chicago 2007).
[166] Kerr, 60 Stan L Rev at 503, 505 (cited in note 164).
[167] Id at 508.
[168] Id at 512.
[169] Id at 522-23.
[170] Flores-Montano, 541 US at 152.
[171] Montoya de Hernandez, 473 US at 534-36.
[172] See notes 151-155 and accompanying text.
[173] Alzahabi, 41 Ind L R at 179 (2008) (cited in note 4).

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 privacy, and this raises a completely different set of issues.[174] 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 government's countervailing interest in extensive border searches. The doctrine was created to control "who and what may enter the country."[175] 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.[176] 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. An officer conducting a Terry stop can pat a person down for weapons, but cannot probe for other contraband.[177] Perhaps the scope of border searches should be limited to keeping out illegal aliens and contraband and not extend to pursuing 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/Bradley Manning, who leaked classified documents to Wikileaks. Based on his activism, House was flagged to be searched at the border when he next left and reentered the country. As a result of this, he was intercepted upon returning from Mexico and his computer was extensively searched. In part because of ACLU intervention, House was able to pursue his claim against the government and ultimately won both an admission of how he had been targeted and an agreement that the seized data be destroyed.[178]

House shows the danger of allowing the government to use the border 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.[179] Neither purpose requires, or is even meaningfully facilitated by, laptop searches.

CONCLUSION

The Fourth Amendment analysis weighs the privacy and dignity interests of the person being searched against the government's need to conduct the search. The government's need can be

---

[174] Alzahabi, 41 Ind L R at 178–79 (2008) (cited in note 4).
[175] Ramsey, 431 US at 620.
[176] Alzahabi, 41 Ind L R at 176 (2008) (cited in note 4); 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).
[177] Terry, 392 US at 27 (1968)
[178] Ryan Gallagher, Government Settles with Researcher Put on Watch List for Supporting Bradly Manning, Slate (May 30, 2013). Available at http://www.slate.com/blogs/future_tense/2013/05/30/david_house_researcher_put_on_watch_list_for_supporting_bradley_manning.html
[179] Ramsey, 431 US at 620.

presumed to be quite strong at the border, so the balance generally tilts in the direction of the state. But theories of the Fourth Amendment generally require some consideration of public attitudes. The data presented here tell us 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. 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 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 carved out an exception for border searches, they did not foresee the smartphone, the laptop home office, sexting, or cloud storage. But it is still worth recalling that the 19th century gave us cases like Boyd v United States, which gave extensive protection to one's personal papers.[180] 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 at the border. Is the government's need for electronic searches in particular great enough to outweigh the dignity and privacy interests that we now know are implicated?

[180] Boyd, 116 US 616 (1886).

Readers with comments should address them to:

Professor Matthew B. Kugler
mkugler@uchicago.edu

Chicago Working Papers in Law and Economics
(Second Series)

For a listing of papers 1–600 please go to Working Papers at http://www.law.uchicago.edu/Lawecon/index.html

601. David A. Weisbach, Should Environmental Taxes Be Precautionary? June 2012
602. Saul Levmore, Harmonization, Preferences, and the Calculus of Consent in Commercial and Other Law, June 2012
603. David S. Evans, Excessive Litigation by Business Users of Free Platform Services, June 2012
604. Ariel Porat, Mistake under the Common European Sales Law, June 2012
605. Stephen J. Choi, Mitu Gulati, and Eric A. Posner, The Dynamics of Contrat Evolution, June 2012
606. Eric A. Posner and David Weisbach, International Paretianism: A Defense, July 2012
607 Eric A. Posner, The Institutional Structure of Immigration Law, July 2012
608. Lior Jacob Strahilevitz, Absolute Preferences *and* Relative Preferences in Property Law, July 2012
609. Eric A. Posner and Alan O. Sykes, International Law and the Limits of Macroeconomic Cooperation, July 2012
610. M. Todd Henderson and Frederick Tung, Reverse Regulatory Arbitrage: An Auction Approach to Regulatory Assignments, August 2012
611. Joseph Isenbergh, Cliff Schmiff, August 2012
612. Tom Ginsburg and James Melton, Does De Jure Judicial Independence Really Matter? A Reevaluastion of Explanations for Judicial Independence, August 2012
613. M. Todd Henderson, Voice versus Exit in Health Care Policy, October 2012
614. Gary Becker, François Ewald, and Bernard Harcourt, "Becker on Ewald on Foucault on Becker" American Neoliberalism and Michel Foucault's 1979 *Birth of Biopolitics* Lectures, October 2012
615. William H. J. Hubbard, Another Look at the Eurobarometer Surveys, October 2012
616. Lee Anne Fennell, Resource Access Costs, October 2012
617. Ariel Porat, Negligence Liability for Non-Negligent Behavior, November 2012
618. William A. Birdthistle and M. Todd Henderson, Becoming the Fifth Branch, November 2012
619. David S. Evans and Elisa V. Mariscal, The Role of Keyword Advertisign in Competition among Rival Brands, November 2012
620. Rosa M. Abrantes-Metz and David S. Evans, Replacing the LIBOR with a Transparent and Reliable Index of interbank Borrowing: Comments on the Wheatley Review of LIBOR Initial Discussion Paper, November 2012
621. Reid Thompson and David Weisbach, Attributes of Ownership, November 2012
622. Eric A. Posner, Balance-of-Powers Arguments and the Structural Constitution, November 2012
623. David S. Evans and Richard Schmalensee, The Antitrust Analysis of Multi-Sided Platform Businesses, December 2012
624. James Melton, Zachary Elkins, Tom Ginsburg, and Kalev Leetaru, On the Interpretability of Law: Lessons from the Decoding of National Constitutions, December 2012
625. Jonathan S. Masur and Eric A. Posner, Unemployment and Regulatory Policy, December 2012
626. David S. Evans, Economics of Vertical Restraints for Multi-Sided Platforms, January 2013
627. David S. Evans, Attention to Rivalry among Online Platforms and Its Implications for Antitrust Analysis, January 2013
628. Omri Ben-Shahar, Arbitration and Access to Justice: Economic Analysis, January 2013
629. M. Todd Henderson, Can Lawyers Stay in the Driver's Seat?, January 2013
630. Stephen J. Choi, Mitu Gulati, and Eric A. Posner, Altruism Exchanges and the Kidney Shortage, January 2013
631. Randal C. Picker, Access and the Public Domain, February 2013
632. Adam B. Cox and Thomas J. Miles, Policing Immigration, February 2013
633. Anup Malani and Jonathan S. Masur, Raising the Stakes in Patent Cases, February 2013
634. Arial Porat and Lior Strahilevitz, Personalizing Default Rules and Disclosure with Big Data, February 2013
635. Douglas G. Baird and Anthony J. Casey, Bankruptcy Step Zero, February 2013
636. Oren Bar-Gill and Omri Ben-Shahar, No Contract? March 2013
637. Lior Jacob Strahilevitz, Toward a Positive Theory of Privacy Law, March 2013
638. M. Todd Henderson, Self-Regulation for the Mortgage Industry, March 2013
639 Lisa Bernstein, Merchant Law in a Modern Economy, April 2013
640. Omri Ben-Shahar, Regulation through Boilerplate: An Apologia, April 2013

641. Anthony J. Casey and Andres Sawicki, Copyright in Teams, May 2013
642. William H. J. Hubbard, An Empirical Study of the Effect of *Shady Grove v. Allstate* on Forum Shopping in the New York Courts, May 2013
643. Eric A. Posner and E. Glen Weyl, Quadratic Vote Buying as Efficient Corporate Governance, May 2013
644. Dhammika Dharmapala, Nuno Garoupa, and Richard H. McAdams, Punitive Police? Agency Costs, Law Enforcement, and Criminal Procedure, June 2013
645. Tom Ginsburg, Jonathan S. Masur, and Richard H. McAdams, Libertarian Paternalism, Path Dependence, and Temporary Law, June 2013
646. Stephen M. Bainbridge and M. Todd Henderson, Boards-R-Us: Reconceptualizing Corporate Boards, July 2013
647. Mary Anne Case, Is There a Lingua Franca for the American Legal Academy? July 2013
648. Bernard Harcourt, Beccaria's *On Crimes and Punishments:* A Mirror of the History of the Foundations of Modern Criminal Law, July 2013
649. Christopher Buccafusco and Jonathan S. Masur, Innovation and Incarceration: An Economic Analysis of Criminal Intellectual Property Law, July 2013
650. Rosalind Dixon & Tom Ginsburg, The South African Constitutional Court and Socio-economic Rights as "Insurance Swaps", August 2013
651. Maciej H. Kotowski, David A. Weisbach, and Richard J. Zeckhauser, Audits as Signals, August 2013
652. Elisabeth J. Moyer, Michael D. Woolley, Michael J. Glotter, and David A. Weisbach, Climate Impacts on Economic Growth as Drivers of Uncertainty in the Social Cost of Carbon, August 2013
653. Eric A. Posner and E. Glen Weyl, A Solution to the Collective Action Problem in Corporate Reorganization, September 2013
654. Gary Becker, François Ewald, and Bernard Harcourt, "Becker and Foucault on Crime and Punishment"—A Conversation with Gary Becker, François Ewald, and Bernard Harcourt: The Second Session, September 2013
655. Edward R. Morrison, Arpit Gupta, Lenora M. Olson, Lawrence J. Cook, and Heather Keenan, Health and Financial Fragility: Evidence from Automobile Crashes and Consumer Bankruptcy, October 2013
656. Evidentiary Privileges in International Arbitration, Richard M. Mosk and Tom Ginsburg, October 2013
657. Voting Squared: Quadratic Voting in Democratic Politics, Eric A. Posner and E. Glen Weyl, October 2013
658. The Impact of the U.S. Debit Card Interchange Fee Regulation on Consumer Welfare: An Event Study Analysis, David S. Evans, Howard Chang, and Steven Joyce, October 2013
659. Lee Anne Fennell, Just Enough, October 2013
660. Benefit-Cost Paradigms in Financial Regulation, Eric A. Posner and E. Glen Weyl, October 2013
661. Free at Last? Judicial Discretion and Racial Disparities in Federal Sentencing, Crystal S. Yang, October 2013
662. Have Inter-Judge Sentencing Disparities Increased in an Advisory Guidelines Regime? Evidence from Booker, Crystal S. Yang, October 2013
663. William H. J. Hubbard, A Theory of Pleading, Litigation, and Settlement, November 2013
664. Tom Ginsburg, Nick Foti, and Daniel Rockmore, "We the Peoples": The Global Origins of Constitutional Preambles, November 2013
665. Lee Anne Fennell and Eduardo M. Peñalver, Exactions Creep, December 2013
666. Lee Anne Fennell, Forcings, December 2013
667. Stephen J. Choi, Mitu Gulati, and Eric A. Posner, A Winner's Curse?: Promotions from the Lower Federal Courts, December 2013

668. Jose Antonio Cheibub, Zachary Elkins, and Tom Ginsburg, Beyond Presidentialism and Parliamentarism, December 2013
669. Lisa Bernstein, Trade Usage in the Courts: The Flawed Conceptual and Evidentiary Basis of Article 2's Incorporation Strategy, November 2013
670. Roger Allan Ford, Patent Invalidity versus Noninfringement, December 2013
671. M. Todd Henderson and William H.J. Hubbard, Do Judges Follow the Law? An Empirical Test of Congressional Control over Judicial Behavior, January 2014
672. Lisa Bernstein, Copying and Context: Tying as a Solution to the Lack of Intellectual Property Protection of Contract Terms, January 2014
673. Eric A. Posner and Alan O. Sykes, Voting Rules in International Organizations, January 2014
674. Tom Ginsburg and Thomas J. Miles, The Teaching/Research Tradeoff in Law: Data from the Right Tail, February 2014
675. Ariel Porat and Eric Posner, Offsetting Benefits, February 2014
676. Nuno Garoupa and Tom Ginsburg, Judicial Roles in Nonjudicial Functions, February 2014
677. Matthew B. Kugler, The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study, February 2014