

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MICHIGAN  
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-20595

v.

Hon. Marianne O. Battani

YUSEF MOHAMMAD RAMADAN,

Defendant.

\_\_\_\_\_ /

**MOTION TO SUPPRESS EVIDENCE SEIZED IN VIOLATION OF  
YUSEF RAMADAN'S FOURTH AMENDMENT RIGHTS**

Defendant Yousef Mohammad Ramadan, by his attorneys Andrew Densemo and Colleen Fitzharris, moves to suppress the evidence seized during the warrantless and suspicionless search of his external hard drive to Fed. R. Crim. P. 12(b)(3)(C) and the Fourth Amendment. In support of this motion, Mr. Ramadan states the following:

1. Mr. Ramadan is charged with two counts of knowing possession of a firearm with an obliterated serial number in violation of 18 U.S.C. § 922(k).
2. On August 15, 2017, Mr. Ramadan and his family boarded a plane bound for Jordan. They planned to move to move to join Mr. Ramadan's family in Israel.
3. When scanning the Ramadans' checked baggage, security agents noticed various tactical equipment and body armor. After making the discovery, the agents contacted the Ramadan family and removed them from the flight.

4. Four federal agents brought Mr. Ramadan to a separate room where he was handcuffed at various times. At some point, the officers physically assaulted Mr. Ramadan.
5. During the interrogation, the agents demanded the passwords and passcodes for the various digital devices (computers, phones, and external hard drives) in the checked luggage. When Mr. Ramadan refused to disclose the passwords and passcodes, the agents began trying to access any digital device they could.
6. Only two devices were accessible without passwords: the external hard drives and thumb drives. The agents found videos and images and questioned Mr. Ramadan about them.
7. The agents subsequently used the information found on the hard drives and Mr. Ramadan's statements in response to questions about the images on the hard drive to apply for a search warrant for all electronic media and a storage unit rented in Mrs. Ramadan's name.
8. The firearms Mr. Ramadan is accused of possessing illegally were found in the storage unit.
9. Although CBP agents have broad authority to perform routine searches at international borders without a warrant or reasonable suspicion, they do not have unbridled authority to detain or search anyone, anything, and in any manner. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 537–41 (1985) (to detain a traveler beyond the scope of a routine border search to monitor bowel movements, CBP

agents must have reasonable suspicion to believe the person is secreting narcotics in their alimentary canal). Instead, the court must always weigh the government's need to search without a warrant against the person's privacy interests.

10. Searches of cell phones implicate significant privacy interests. Before searching data on cell phones, "officers must generally secure a warrant." *Riley v. California*, 134 S. Ct. 2473, 2485 (2014). "[C]ell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* at 2488–89. Nowadays, cell phones store contact information, email, photos, banking information, health records, maps, GPS data, Internet browsing history, purchase receipts—and the list goes on and grows constantly. *Id.* at 2489–91. In short, a cell phone can help government officials reconstruct "[t]he sum of an individual's private life." *Id.* at 2489. The government's need "to regulate the collection of duties and to prevent the introduction of contraband into this country," *Montoya de Hernandez*, 473 U.S. at 538, pales in comparison to the privacy interests undermined by a free-for-all search of a person's phone.

11. To protect these privacy interest, CBP agents must obtain a warrant to search a phone or, at the very least, have reasonable suspicion to believe contraband will be found on the phone before they may scour its digital contents.

12. Because CBP agents searched Mr. Ramadan's phone without a warrant or reasonable suspicion, they violated the Fourth Amendment, and therefore the

evidence seized must be suppressed as the fruits of an unlawful search. *See Wong Sun v. United States*, 371 U.S. 471, 484 (1963).

13. All statements Mr. Ramadan made to the police about the videos and photos found on the hard drives are fruits of the illegal search and must be suppressed. *Wong Sun*, 371 U.S. at 486. Paragraphs 8, 10–11, and 14–18 of the affidavit for a search warrant are fruits of the illegal search because the agents asked Mr. Ramadan about the location of firearms depicted in the photos found on the hard drive. (*See Ex. A, Search Warrant.*)

14. The Assistant U.S. Attorney assigned to this case does not concur in this motion.

### **CONCLUSION**

CBP officers searched Mr. Ramadan's cell phone without a warrant or reasonable suspicion to believe evidence of criminal activity was on the phone. All fruits seized during that warrantless, suspicionless search must therefore be suppressed.

Dated: October 25, 2017

Respectfully Submitted,

FEDERAL DEFENDER OFFICE

s/Andrew Densmo  
andrew\_densmo@fd.org

s/Colleen P. Fitzharris  
colleen\_fitzharris@fd.org  
Attorneys for Defendant  
613 Abbott St., 5th Floor  
Detroit, MI 48226  
Phone: 313-967-5542

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MICHIGAN  
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-20595

v.

Hon. Marianne O. Battani

YOUSSEF MOHAMMAD RAMADAN,

Defendant.

---

**BRIEF IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE**

Although the government enjoys broad authority to take reasonable measures for the narrow purpose of enforcing immigration and customs laws, Customs and Border Patrol (“CBP”) officers do not have free reign at the border to search anything in any way they see fit. Cell phones, computers, hard drives, flash drives, and DVDs store extraordinary quantities of information ranging “from the mundane to the intimate,” *Riley v. California*, 134 S. Ct. 2473, 2490 (2014), meaning that any examination of a computer or phone has the potential to expose “many sensitive records previously found in the home” and “a broad array of private information never found in a home in any form,” *id.* at 2491. Given the extraordinary quantity and quality of sensitive information border agents may uncover during any search of a cell phone, searches of digital devices implicate significant privacy interests. To protect these privacy interests adequately, government agents must have some level of suspicion before searching a

phone at the border for the purpose of stopping the import of contraband. The CBP agents who seized and searched Mr. Ramadan's hard drives, cell phones, and computers had no information to conclude reasonably that they would contain contraband. All evidence discovered during that search must therefore be suppressed, as well as any evidence later garnered as a fruit of this unlawful search.

### **I. BACKGROUND**

On August 15, 2017, Yousef Ramadan, his wife, and his four children boarded a plane to travel to Jordan. From there, they planned to fly to Israel, where they intended to settle down so that Mr. Ramadan could care for his aging father. Mr. Ramadan checked a few bags. While x-raying the checked bags, TSA agents noticed armor, a taser, taser cartridges, a rifle scope, pepper spray, and two-way radios packed in some of the suitcases. Also in the checked luggage were three computers, a hard drive, five external hard drives, digital cameras, a DVD, a sim card, and four I-phones. CBP officers decided to pull Mr. Ramadan and his family from the plane for further questioning.

Each member of the Ramadan family was separated into different rooms. No CBP officer read Mr. Ramadan his *Miranda* rights, and yet they began questioning him about the contents of his luggage and travel plans. At some point during this questioning, the officers physically assaulted Mr. Ramadan and placed him in handcuffs. Mr. Ramadan asked for an attorney and for the interrogation to be recorded. The agents refused both requests. The agents demanded that he tell them the passwords and passcodes to unlock the cell phones and computers. When he refused to provide such

information, the agents told Mr. Ramadan that he had no choice but to turn over that information.

Frustrated by Mr. Ramadan's refusal to disclose his passwords and passwords or to grant access to the digital devices, the CBP agents tried to review the electronic media in any way they could. Only the external hard drives and flash drives were accessible. During the search of these external hard drives, the agents discovered videos and photos they believed were ISIS propaganda videos, photographs of firearms and explosives.

After viewing the photos and videos on the external hard drives, the agents questioned Mr. Ramadan about the contents of the various media, whether he knew how to make pipe bombs, and whether he supported the mission of ISIS. In response, Mr. Ramadan made incriminating statements.

## **II. LEGAL STANDARD**

The Fourth Amendment requires that all searches and seizures of "persons, houses, papers, and effects" be reasonable. U.S. Const. amend. IV. "Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant" supported by probable cause. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995). A warrantless search is reasonable "only if it falls within a specific exception to the warrant requirement." *Riley*, 134 S. Ct. at 2482.

When weighing the reasonableness of a search, courts must first decide whether the search was performed to discover evidence of wrongdoing. If the purpose of the search is to perform an ordinary criminal investigation, then law enforcement officers must get a warrant. *Vernonia Sch. Dist.*, 515 U.S. at 653. “[W]hen special needs, beyond the need for law enforcement, make the warrant and the probable-cause requirement impracticable,” a search without a warrant or probable cause may be reasonable. *Id.* Courts “determine whether to exempt a given type of search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *Riley*, 134 S. Ct. at 2484 (internal quotation marks omitted). Any exception to the warrant requirement must be tethered to the justifications underlying the exception to the warrant requirement. *Id.* at 2485.

### III. DISCUSSION

#### **A. At a minimum, CBP agents must have reasonable suspicion to conduct any type of search of a digital device at the border.**

In *Riley*, the Supreme Court considered whether the nature of cell phones alters the government’s need to conduct a warrantless search incident to an arrest. *See* 134 S. Ct. at 2488–91. The Court weighed the privacy interests people have in their cell phone, *see id.* at 2489–91, against the government’s need to search a phone during an arrest to protect officer safety and to preserve evidence, *see id.* at 2485–89. On balance, the Court concluded that even though arrestees have a reduced expectation of privacy, these two

government interests do not justify the warrantless search of a cell phone. *Id.* at 2495. This is so because digital devices contain “far *more* [information] than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.” *Id.* at 2491.

This Court should similarly find the government’s interests at the border are not so great that a warrant would undermine CBP’s ability to secure the border effectively. Although “the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border,” *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985), the sheer quantity and quality of information available on digital devices therefore tips the balance in favor of greater privacy protections. Accordingly, “the answer to the question of what police must do before searching a cell phone seized” at the border should be “simple—get a warrant.” *Riley*, 134 S. Ct. at 2495. At the very least, border agents must have reasonable suspicion to believe contraband will be found on the phone.

*1. People store very personal information on their cell phones.*

U.S. citizens and foreign nationals possess extraordinary personal information stored on their cell phones, tablets, and computers.<sup>1</sup> Gone are the days when people

---

<sup>1</sup> Ninety-five percent of Americans carry a cell phone of some kind, and 77% own a smartphone. (Ex. C, Pew Research Center: Internet, Science & Technology,

could carry on that which fit into the confines of a suitcase, briefcase, or purse. Before the advent of modern digital devices, searches at the border were “limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.” *Id.* at 2489. Not so anymore. Digital devices are as different from suitcases as “a ride on horseback” and “a flight to the moon.” *Id.*

“Cell phones” and other digital devices “differ in both a quantitative and a qualitative sense from other objects that might be kept on [a border-crosser’s] person.” *Id.* To start, they may be used as “cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.” *Id.* The storage capacity of a cell phone, computer, or external hard drive is not limited by the size of phone. Consumers may purchase the latest version of the iPhone 8 with a storage capacity of 64 gigabytes (and up to 256 gigabytes), (Ex. B, iPhone 8, <https://www.apple.com/iphone-8/specs/> (last visited Oct. 25, 2017))—more than double the storage capacity of the standard smart phone on the market at the time *Riley* was decided, *see id.* at 2489 (noting “the current top-selling smart phone has a standard capacity of 16 gigabytes”). If “[s]ixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos,” *Riley*, 134 S. Ct. at 2489, 256 gigabytes likely translates to trillions.

---

*Demographics of Mobile Device Ownership and Adoption in the United States* (Jan. 17, 2017).) Between 2013 and 2014, smartphone ownership in the U.S. increased by six percent. (Ex. D, Deloitte, Digital Democracy Survey 5 (2015).) U.S. consumers reported valuing their smartphones more than all other digital devices. (*Id.* at 6.)

The extraordinary storage capacity of digital devices raises several privacy concerns. First, they collect many different and distinct types of information—bank statements, videos, GPS location, Internet browsing history, etc. *Id.* Second, the amalgamation of these various data points and documents can help the government reconstruct “the sum of an individual’s private life.” *Id.* Third, digital devices collect and store information over a significant period of time beginning at the device’s creation. *See id.* Fourth, thousands of applications and programs allow users to store a host of private information—medical records, insurance information, bank statements, and credit scores. *See id.* at 2490. Fifth, the historic location information stored on a digital device potentially allows law enforcement officers to pinpoint the owner’s movements down to the minute, *id.*, and his or her “familial, political, professional, religious, and sexual associations,” *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). In other words, unlike a search of an international traveler’s suitcase, which reveals “only what the bag contained on the current trip,” a search of a digital device could reveal “everything it had ever carried.” *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (en banc).

A cell phone’s ability to connect to cloud-based storage further underscores the extent of the privacy interests at stake when law enforcement officers search electronic devices. The availability of cloud-based storage causes the analogy between digital devices and storage containers to “crumble[] entirely” because cloud computing expands the device’s storage capacity and potentially extends a search “well beyond

papers and effects in the physical proximity” of the border crosser. *Riley*, 134 S. Ct. at 2491. Indeed, some users even use their digital devices as security cameras to monitor the interior of their homes.

Finally, these privacy concerns are not merely academic; research subjects report “see[ing] the intrusiveness of electronic-device searches as comparable to that of strip searches and body cavity searches.” (Ex. E, Matthew B. Kugler,<sup>2</sup> Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. Chi. L. Rev. 1165, 1167, 1194–96 (2014)) (describing 300 participants’ views of the intrusiveness of strip searches, digital-device, and searches of a car gas tank). Respondents also stated that a search of a digital device would reveal more information than a strip search. *Id.* at 1209.

In sum, digital devices “contain (1) many kinds of data, (2) in vast amounts, and (3) corresponding to a long swath of time.” *United States v. Lichtenberger*, 786 F.3d 478, 488 (6th Cir. 2015). *Riley* makes plain that digital devices are different than any other personal item an international traveler may carry. And a search of a cell phone,

---

<sup>2</sup> Professor Krugler conducted an extensive study of how people perceive the intrusiveness of a digital-device search. Ultimately, he concludes a reasonable-suspicion standard would be a modest approach to protect the private information on the phone. Krugler, *supra*, at 1211. He suggests, however, that a higher level of suspicion may be the better approach or that courts should narrowly limit border searches to the exclusion of physical contraband and undesired persons, which would eliminate the need to search electronic devices altogether. *See id.* at 1207–10.

computer, or digital storage device “greatly increases the potential privacy interests at stake, adding weight to one side of the scale while the other remains the same.” *Id.*

2. *The government’s need to search digital devices at the border without a warrant is limited.*

The Supreme Court has noted that the border exception was “like the similar search incident to lawful arrest exception” because historical practice—not exigency—guided the practice. *United States v. Ramsey*, 431 U.S. 606, 621 (1977) (internal quotation marks omitted). There are two justifications for warrantless and suspicionless searches at the border: (1) to identify those who qualify to enter the country; and (2) to ensure the traveler’s belongings are “effects which may be lawfully brought in.” *Carroll v. United States*, 267 U.S. 132, 154 (1925); *Montoya de Hernandez*, 473 U.S. at 537 (searches at the border serve the purpose of “regulat[ing] the collection of duties and . . . prevent[ing] the introduction of contraband into this country”). The government may not, however, use border searches to investigate and uncover criminal wrongdoing because doing so would “untether” the justifications for the warrant exception from the government’s legitimate interests. *See Riley*, 134 S. Ct. at 2485; *see also Florida v. Royer*, 460 U.S. 491, 500 (1983) (warrantless searches “must be limited in scope to that which is justified by the particular purposes served by the exception”).

Accordingly, border agents may invoke these interests to prevent undocumented immigrants from entering the country, *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973), and regulating the goods imported into the country, *see United States v. Thirty-*

*Seven Photographs*, 402 U.S. 363, 376 (1971) (luggage may be inspected to “exclud[e] illegal articles”); *Montoya de Hernandez*, 473 U.S. at 537 (to prevent smuggling of narcotics). Each of “the[se] justifications for the exception to the warrant requirement are generally framed in terms of threats posed at the point of entry.” *United States v. Kim*, 103 F. Supp. 3d 32, 56 (D.D.C. 2015).

3. *On balance, the traveler’s privacy interests in a digital device outweigh the government’s need to perform a suspicionless search at the border.*

The fact that those who seek entry to the United States have diminished expectations of privacy “does not mean that the Fourth Amendment falls out of the picture entirely.” *Riley*, 134 S. Ct. at 2488. “[W]hen ‘privacy-related concerns are weighty enough’ a ‘search may require a warrant, notwithstanding the diminished expectations of privacy of the [person searched].’” *Id.* (quoting *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013)). People in custody have diminished privacy expectations, as well, but “[n]ot every search ‘is acceptable solely because a person is in custody.’” *Id.* (quoting *King*, 133 S. Ct. at 1979). Probationers similarly do not expect the government to honor their privacy interests to the same degree as others. *United States v. Lara*, 815 F.3d 605, 612 (9th Cir. 2016). Yet the Ninth Circuit concluded a probationer’s privacy interest in his cell phone was sufficiently weighty to require procurement of a warrant before a search. *Id.*

Similarly, international travelers seeking entry to the United States do not abandon their well-founded expectation of privacy in the contents of their digital

devices. As discussed previously, a travelers' privacy-related concerns on a cell phone or computer are substantial. And, while the government's interest in customs and immigration enforcement is significant, the balance must ultimately tip in favor of privacy protections.

a. The limits on border searches.

A brief review of when suspicionless and warrantless searches are permissible at the border is helpful to understand the boundaries of the government's power to search at the border. In *Ramsey*, 431 U.S. at 623, the Supreme Court held that border agents do not need probable cause or a warrant to open an envelope at the border to search for contraband. The Supreme Court condoned border patrol's practice of removing, disassembling, and reassembling a car's fuel tank without any suspicion at all. *United States v. Flores-Montano*, 541 U.S. 149, 155 (2004). Although the Court recognized such a search inconvenienced international travelers, it concluded the invasion of privacy was minimal because a fuel tank is not the repository of personal information; it is the repository of fuel. *Id.* at 154.

In contrast, the Supreme Court has sanctioned "the detention of a traveler at the border, beyond the scope of a routine customs search and inspection," who border agents "reasonably suspect [of] smuggling contraband in her alimentary canal." *Montoya de Hernandez*, 473 U.S. at 541. To engage in this practice, the border agent must be able to articulate "a particularized and objective basis for suspecting the particular person of alimentary canal smuggling." *Id.* at 541–42. Critically, the border agent must have

reasonable suspicion to believe contraband might enter the country, not that the object to be searched might contain evidence of criminal activity. *See id.* at 537 (nothing border agents are tasked with collecting duties and preventing the introduction of contraband into the country); *id.* at 541 (the border agent must “reasonably suspect that the traveler is smuggling contraband”). This standard is appropriate because the government has an interest in halting the importation of narcotics at the border, and “this type of smuggling gives no external signs and inspectors will rarely possess probable cause to arrest or search.” *Id.* at 541.

The holding of *Montoya de Hernandez* is limited to prolonged detention; the Court expressly did not address “what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches.” *Id.* at 541 n.4. Since *Montoya de Hernandez*, circuit courts have concluded reasonable suspicion is required to perform “strip searches, alimentary canal searches, x-rays, and [to] remov[e] . . . an artificial limb.” *United States v. Kolsuz*, 185 F. Supp. 3d 843, 853 & n.14 (E.D. Va. 2016) (collecting cases). To determine whether a search is so intrusive as to require heightened suspicion, courts consider how the intrusive search will undermine a person’s dignity and how much information about the person the search will reveal. *United States v. Vega-Bravo*, 729 F.2d 1341, 1345–49 (11th Cir. 1984) (concluding a person retains his or her dignity during an x-ray, but reveals sensitive information, and therefore reasonable suspicion is required to perform the search).

b. Border searches of cell phones.

Since the Supreme Court authored *Riley* only a handful of district courts have balanced the unique privacy concerns raised by a search of a cell phone against the government's national-security interests at the border. Two courts in this district were asked only to decide whether a warrant was required to search a cell phone at the border, *United States v. Serhan*, No. 14-20685, 2015 WL 3578744, at \*2–3 (E.D. Mich. June 5, 2015) (Hood, C.J.), or whether a warrant was required to perform a forensic analysis at another location, *United States v. Feiten*, No. 15-20631, 2016 WL 894452, at \*4–7 (E.D. Mich. Mar. 9, 2016) (Cleland, J.). In both instances, the district courts concluded no warrant was required, but there was no indication the defendants argued that reasonable suspicion was required instead. *See Serhan*, 2015 WL 3578744, at \*2–3 (“Serhan claims that the border agents’ search of his private data and communications required a search warrant.”); *Feiten*, 2016 WL 894452, at \*2 (“[The defendant] urges the court to expand . . . *Riley* . . . , and find all warrantless searches of electronic devices at the border unconstitutional.” (citation omitted)).

Most courts have concluded border agents must have reasonable suspicion to believe contraband was on a digital device to conduct a “forensic search” of a traveler’s cell phone or digital device seized at the border because of the quantity of highly sensitive information found on cell phones. *Kolsunz*, 185 F. Supp. 3d at 859 (“[A] nonroutine border search of a cell phone is constitutional if it is supported by reasonable suspicion.”); *Kim*, 103 F. Supp. 3d at 57 (“[W]herever the Supreme Court or the Court of Appeals eventually draws the precise boundary of a routine border search

... this search ... was unreasonable given the paucity of grounds to suspect that criminal activity was in progress.”); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 568–70 (D. Md. 2014) (requiring reasonable suspicion to conduct a border search). Only one district court has concluded no suspicion is required to conduct a forensic search off-site. *Feiten*, 2016 WL 894452, at \*7.<sup>3</sup>

Mr. Ramadan acknowledges that some district courts have concluded border agents do not even need reasonable suspicion to conduct a manual search at the border. *Kolsuz*, 185 F. Supp. 3d at 855 (“[T]he manual search of defendant’s iPhone conducted at the airport was a routine border search that did not require individualized suspicion.”); *United States v. Caballero*, No. 15CR2738, 2016 WL 1546731, at \*1 (S.D. Cal. Apr. 14, 2016) (“The Court finds that it is bound by Ninth Circuit authority on the border search doctrine which permits law enforcement at the international border to

---

<sup>3</sup> The *Feiten* court rested its conclusion on the false premise that digital devices are just like containers that cross the border, 2016 WL 894452, at \*6—a comparison the Supreme Court resoundingly rejected, *Riley*, 134 S. Ct. at 2491 (“Treating a cell phone as a container whose contents may be searched incident to arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere . . . .” (citation omitted)). In addition, the *Feiten* court claimed customs agents should be permitted to search any digital device that crosses the border to prevent the importation of child pornography because “most child pornography crimes involve the use of a computer.” 2016 WL 894452, at \*6. True as that statement may be, that fact alone does not support the court’s conclusion. Smugglers frequently secrete narcotics in their alimentary canals, see *Montoya de Hernandez*, 473 U.S. at 538–39, and yet border agents must have reasonable suspicion to detain a suspected smuggler until she passes her bowels, *id.* at 541. The mere fact that a particular type of contraband is smuggled in a particular way does not relieve border agents of the responsibility to have some suspicion to conduct an invasive search.

perform a cursory search of a digital device upon something less than reasonable suspicion without violating the Fourth Amendment.” (citing *Cotterman*, 709 F.3d at 956–57)). This court should conclude otherwise.

c. The distinction between “forensic” and “routine” digital searches is meaningless.

The few courts to address whether border agents must have some level of suspicion to search a digital device have drawn a distinction between “forensic” searches and “conventional,” manual searches at the border. One district court defined a “forensic” search as a search that occurs “when a computer expert creates a bitstream copy and it analyzes it by means of specialized software.” *Saboonchi*, 990 F. Supp. 2d at 569.

The genesis of this distinction lies in the Ninth Circuit’s *Cotterman* opinion. In *Cotterman*, the en banc court considered what level of suspicion a border agent would need to conduct a “forensic examination” of a computer seized at the border. *Cotterman*, 709 F.3d at 960. Border agents seized the defendant’s two computers and three video cameras after discovering he was a registered sex offender. *Id.* at 957. During the secondary inspection, border agents learned that law enforcement officers believed the defendant was involved in “some type of child pornography.” *Id.* This information prompted the agents to begin searching the defendant’s computers and cameras for evidence of child pornography. *Id.* at 958. When they encountered password-protected files, the agents decided to transport the digital devices to an ICE office to use forensic

software to copy the hard drives and crack the code to the password-protected files. *Id.* at 958–59. The defendant did not challenge the initial border search (after all, no evidence of criminal activity was discovered), but instead challenged the legality of the “forensic examination” at the ICE facility. *See id.* at 959.

In this context, and without *Riley*’s guidance, the Ninth Circuit issued the following unprompted remark: “the initial search of Cotterman’s electronic devices at the border is not in doubt.” *Id.* at 960. In doing so, the court established a distinction between the practice of powering up a device and scanning it for evidence of pornography and a so-called “forensic” examination.

In *Saboonchi*, the district court followed the Ninth Circuit’s lead, concluding a “forensic” search at the border requires reasonable suspicion. 990 F. Supp. 2d at 569–70; *see also Kolsuz*, 185 F. Supp. 3d at 850–59 (treating a manual search of a phone as “routine,” but a forensic search as “non-routine” and therefore subject to a reasonable-suspicion requirement); *Kim*, 103 F. Supp. 3d at 57 (treating “routine” searches differently from “forensic” searches). The district court believed “conventional” computer searches “can be analogized to a conventional search of a suitcase” in that it “has the same inherent limitations—and the same inherent risk of invasiveness—irrespective of what is being searched,” namely the amount of time a CBP agent has to review the files. *Saboonchi*, 990 F. Supp. 2d at 564. And a “conventional” search leaves the digital device intact. *Id.* at 568.

But this Court is not bound by those opinions and should not follow them. First, nothing in *Riley* suggests the search method makes a difference. Indeed, quite the opposite. In *Riley*, a police officer seized the defendant's smartphone incident to an arrest and began scrolling through the text messages and contact lists. 134 S. Ct. at 2480. In the companion case to *Riley*, police officers seized the defendant's flip phone and began looking at his call activity and the photo he used for his background. *Id.* at 2481. In both instances, the Supreme Court concluded these warrantless, manual searches violated the Fourth Amendment without any discussion of "forensic searches." *See id.* at 2492–93 (rejecting the contention that police officers may always manually search a call log without a warrant because "call logs typically contain more than just phone numbers; they include any identifying information that an individual might add").<sup>4</sup> Thus, whether a search is reasonable "does not turn on the application of an undefined term like 'forensic,'" but instead requires conducting a careful balance between privacy and government interests. *Kim*, 103 F. Supp. 3d at 55.

Second, there is no factually meaningful difference between manual and forensic searches, which both lay bare the sensitive information stored on a digital device. The act of manually tapping on and searching through a person's photos, call log, email, and

---

<sup>4</sup> The *Saboonchi* court acknowledged the Court found non-forensic digital searches unconstitutional. *United States v. Saboonchi*, 48 F. Supp. 3d 815, 819 (D. Md. 2014) (hereinafter "*Saboonchi II*"). But the district court never had cause to revisit its prior conclusion that reasonable suspicion was required to perform a forensic search because *Riley* supported the district court's prior conclusion. *See id.*

applications is still immensely invasive. And, at least one district court has suggested, this process may be more invasive than using a software program to create thumbnail previews of the pictures and videos on a computer. *See Feiten*, 2016 WL 894452, at \*6 (“The OS Triage [software] is actually *less* invasive of personal privacy than is a search done by hand.”). In addition, a manual search of a cell phone or computer may “alter key evidentiary aspects of each file inspected, such as the date and time the file was last viewed.” *Id.*

This Court should decline to distinguish between a manual and forensic search at the border.

d. *Riley* requires some level of suspicion to search a digital device at the border.

*Riley* explains and scientific research demonstrates “searches of electronic devices,” including cell phones, “invoke privacy and dignity concerns to the same extent as body cavity and strip searches” and home. *Kugler, supra*, at 1208; *Riley*, 134 S. Ct. at 2491 (“[A] cell phone search would typically expose to the government far *more* than the most exhaustive house search . . . .”). And, “when it comes to the Fourth Amendment, the home is first among equals,” *Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013), in part because of the intimate details about a person’s life contained therein. Thus, at the very least, border agents must have reasonable suspicion to believe the digital device contains contraband or information about why a person is ineligible for entry. *See Kim*, 103 F. Supp. 3d at 556–57 (“[T]he national security concerns that

underlie the enforcement of export control regulations at the border must be balanced against the degree to which [the defendant's] privacy was invaded in this instance.”).

The unique features of digital devices suggest they are as invasive as searches of alimentary canals. To start, while rectal or strip searches are invasive and dehumanizing,<sup>5</sup> the searcher can uncover very little personal information about a person from that search alone. In stark contrast, a digital device search reveals substantially more about the owner's private life. Once a person's dignity and privacy interest have been invaded, “the exposure of confidential and personal information has permanence. It cannot be undone.” *Cotterman*, 709 F.3d at 966. In short, although a cell phone search, “lacks the discomfort or embarrassment that accompanies a body-cavity search, it has the potential to be even more revealing.” *Saboonchi*, 990 F.Supp.2d at 568.

What that means is a search of a cell phone, computer, or external hard drive is analogous to the search of a home, which requires any law enforcement agent to get a warrant. Accordingly, to search a digital device at the border, CBP agents should get a warrant or have probable cause.<sup>6</sup>

---

<sup>5</sup> To be clear, the Supreme Court has never weighed in on the question whether reasonable suspicion is the appropriate level of suspicion required to perform a strip or rectal search at the border. *See Montoya de Hernandez*, 473 U.S. at 541 n.4.

<sup>6</sup> The government may argue *United States v. Stewart*, 729 F.3d 517, 525 (6th Cir. 2013), forecloses Mr. Ramadan's argument. In *Stewart*, the Sixth Circuit concluded a search the defendant's laptop computer that began at the airport and continued at an ICE facility twenty minutes away was not an extended border search requiring reasonable suspicion of criminal activity. *Id.* at 525–26. The *Stewart* court did not have the benefit of *Riley*, which the Supreme Court issued nearly a year later. *Compare Stewart*, 729 F.3d 517 (issued in September 3, 2013), *with Riley*, 134 S. Ct. 2473 (issued June 25, 2014).

**B. Searches that potentially chill freedom of speech and association require heightened suspicion.**

The First Amendment protects not only the right to speak, but also a person's "right to receive information and ideas," *Stanley v. Georgia*, 394 U.S. 557, 564 (1969), "freedom of inquiry," *Griswold v. Connecticut*, 381 U.S. 479, 482 (1965), and right to browse and purchase expressive materials anonymously, without fear of government discovery, *see, e.g., McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995); *Lamont v. Postmaster Gen.*, 381 U.S. 301, 307 (1965). In addition, the First Amendment protects a person's freedom of association, and any government "action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny." *N.A.A.C.P. v. Alabama ex rel. Patterson*, 357 U.S. 449, 460–61 (1958). Compelled disclosure of information that may reveal a person's associations threatens the right to association. *See id.* at 462.

Digital devices contain numerous expressive materials. Emails, ebooks, electronic magazine articles, photographs, and videos are classic examples of materials the First Amendment protects. Digital devices contain additional expressive materials—a person's browsing, searching, and purchasing histories reveal much about a person's fleeting questions and established interests. An agent manually searching a person's digital device may uncover the owner's reading habits and associations. Scrolling through emails may reveal political donations, group memberships, or even whether the person attends church regularly. Access to bank accounts tells law

enforcement agents about political and charitable donations. GPS data might reveal if a cell phone's owner "is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about [that] person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010).

The Supreme Court has long recognized that courts must approach searches and seizures of content that implicates First Amendment concerns with great care to ensure the search does not chill those rights. *See New York v. P.J. Video, Inc.*, 475 U.S. 868, 873–74 (1983) (describing the judicial safeguards required to seize films and books). Government agents need probable cause to seize such expressive materials, *id.* at 875, and "[w]here the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with scrupulous exactitude," *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (internal quotation marks omitted). These basic protections—review by a neutral magistrate, probable cause, and a particularized description of the place to be searched and the things to be seized—are critically important safeguards to constrain arbitrary enforcement and to protect First Amendment rights. *See id.* at 566–67. The right to express ideas and associate with others does not vanish at the border. A warrant—or at least reasonable suspicion—strikes the appropriate balance.

**C. CBP officers did not have reasonable suspicion to search Mr. Ramadan's phone for any reason.**

In many respects the level of suspicion required to search a cell phone at the border is academic because the border agents did not even have reasonable suspicion to believe they would find contraband on Mr. Ramadan's digital devices. CBP officers may not rely on a hunch that contraband might be on the phone; they must be able to "point to 'specific and articulable facts, which taken together with rational inferences from those facts,' reasonably suggest that" contraband or customs-related information will be found on the external hard drive. *United States v. Urrieta*, 520 F.3d 569, 573 (6th Cir. 2008) (quoting *Terry v. Ohio*, 392 U.S. 1, 21 (1968)).

By the time the CBP agents decided to conduct a media review, they had limited information about Mr. Ramadan. They knew that he and his family were moving to Israel to join Mr. Ramadan's aging parents. They knew that Mr. Ramadan had tactical gear, but no firearms.<sup>7</sup> And they knew that Mr. Ramadan was an aspiring documentary filmmaker who hoped to produce a film about the conflict in the West Bank. At the time they started searching Mr. Ramadan's phone, they did not have any reason to believe he supported any terrorist organizations. Nor did they have any reason to conclude Mr. Ramadan stored any information connected to any crime under investigation stored on his external hard drive. At best, the agents repeatedly mentioned Mr. Ramadan's unwillingness to disclose the passcodes and passwords to the various devices. But a person's refusal to disclose information of any kind cannot suffice to

---

<sup>7</sup> The government has not charged Mr. Ramadan with any crimes for his possession of the items found in his checked luggage.

create reasonable suspicion. *Cf. Cotterman*, 709 F.3d at 969 (“[P]assword protection of files, in isolation, will not give rise to reasonable suspicion . . .”).

The agents did not have any reason to believe contraband or customs-related information would be found on Mr. Ramadan’s external hard drive. Accordingly, the warrantless, suspicionless search of the drives was unreasonable and unconstitutional.

**D. Mr. Ramadan’s statements in response to questions about the photos and videos on the hard drive are fruits of the illegal search.**

“The exclusionary rule generally bars the admissibility at trial of tangible evidence, as well as verbal statements, acquired through unconstitutional means.” *United States v. Akridge*, 346 F.3d 618, 623 (6th Cir. 2003). This basic premise finds its origins in *Wong Sun*, when the Supreme Court first coined the expression “fruit of the poisonous tree.” *Oregon v. Elstad*, 470 U.S. 298, 306 (1985). In *Wong Sun*, the defendant made statements to the police after they had illegally entered his home and arrested him. 371 U.S. at 486. The Court concluded that “the policies underlying the exclusionary rule [do not] invite any logical distinction between physical and verbal evidence.” *Id.* For that reason, “verbal evidence which derives so immediately from an unlawful entry and an unauthorized arrest . . . is no less the ‘fruit’ of official illegality than the more common tangible fruits of the unwarranted intrusion,” *i.e.*, tangible materials obtained during the search. *Id.* at 485. “[T]he indirect fruits of an illegal search or arrest should be suppressed when they bear a sufficiently close relationship to the underlying illegality.” *New York v. Harris*, 495 U.S. 14, 19 (1990).

To determine whether to suppress confessions made after an illegal search should consider the policy interests of the Fourth Amendment. *Brown v. Illinois*, 422 U.S. 590, 602 (1975). *Miranda* warnings do not “attenuate the taint of an unconstitutional arrest” or search, but the fact that they were given is one factor to consider when deciding whether the statements are the product of free will. *Id.* at 602–03. The court should also consider intervening circumstances and the flagrancy of the police misconduct. *Id.* at 603–04. “[T]he burden of showing admissibility rests, of course, on the prosecution.” *Id.* at 604.

**E. The search warrant for the storage unit is fruit of the illegal search.**

Evidence of any type that can be traced back to an illegal search is a fruit, including statements in an application for a search warrant. *See Wong Sun v. United States*, 371 U.S. 471, 484 (1963). The key to the inquiry is whether law enforcement officers used the products of the illegal search to obtain the evidence validly. *See Murray v. United States*, 487 U.S. 533, 542 (1988) (“The ultimate question, therefore, is whether the search pursuant to warrant was in fact a genuinely independent source of the information and tangible evidence at issue here.”). If allegations in a search warrant are the product of an illegal search, the court must excise the tainted portions and then assess whether the warrant still establishes probable cause. *United States v. Robertson*, 239 F. Supp. 3d 426, 459 (D. Conn. 2017) (citing *Murray*, U.S. at 542); *United States v. Martinez*, 696 F. Supp. 2d 1216, 1245 (D.N.M. 2010) (citing *United States v. Sims*, 428 F.3d 945, 954 (10th Cir. 2005)).

Paragraphs 8, 10–11, and 14–18 of the affidavit are fruits of the illegal search because the agents used the information gathered from the search of the external hard drive to interrogate Mr. Ramadan about terrorist organizations and the firearms shown in the photographs. Without those averments, the warrant does not establish probable cause to search the storage locker or the electronic devices.

## **V. CONCLUSION**

The border agents' suspicionless and warrantless search of Mr. Ramadan's phone violated the Fourth Amendment. All fruits seized as a result of that search must therefore be suppressed.

Dated: October 25, 2017

Respectfully Submitted,

FEDERAL DEFENDER OFFICE

s/Andrew Densmo  
andrew\_densmo@fd.org

s/Colleen P. Fitzharris  
colleen\_fitzharris@fd.org

Attorneys for Defendant  
613 Abbott St., 5th Floor  
Detroit, MI 48226  
Phone: 313-967-5542

### **CERTIFICATE OF SERVICE**

Counsel certifies that on the above date, the foregoing paper was filed with the clerk of the Court using the ECF system, which will send notification to opposing counsel.

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MICHIGAN  
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-20595

v.

Hon. Marianne O. Battani

YUSEF MOHAMMAD RAMADAN,

Defendant.

\_\_\_\_\_ /

**INDEX OF EXHIBITS**

- Exhibit A:** Search Warrant
- Exhibit B:** iPhone 8, <https://www.apple.com/iphone-8/specs/> (last visited Oct. 25, 2017)
- Exhibit C:** Pew Research Center: Internet, Science & Technology, *Demographics of Mobile Device Ownership and Adoption in the United States* (Jan. 17, 2017)
- Exhibit D:** Deloitte, *Digital Democracy Survey* (2015)
- Exhibit E:** Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. Chi. L. Rev. 1165, 1167, 1194–96 (2014)

# EXHIBIT A

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Michigan

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Devon Storage locker and various electronic devices more  
fully described in Attachment A.


Case: 2:17-mc-51175 - 1  
Case No. Judge: Borman, Paul D.

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Michigan.  
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A..

I hereby certify that the foregoing is a certified copy of the original on file in this office.	
Clerk, U.S. District Court Eastern District of Michigan	
By: <u>s/Carolyn Ciesla</u>	
Deputy	

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B.

**YOU ARE COMMANDED** to execute this warrant on or before September 6, 2017 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

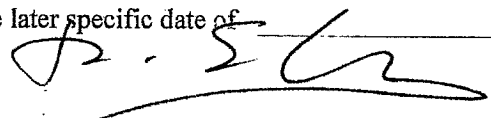
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.  
(United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☒ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued: 8/23/17 1:27 pm

City and state: Detroit, MI

  
\_\_\_\_\_  
Judge's signature  
R. Steven Whalen, U. S. Magistrate Judge  
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

## Return

Case No.:

2:17-MC-51175-1

Date and time warrant executed:

8/23/2017 3:01 PM EST

Copy of warrant and inventory left with:

INSIDE STORAGE UNIT B64 4750 STATE RD. NW  
AR 304 MI

Inventory made in the presence of:

SA DAVID BANACH

Inventory of the property taken and name of any person(s) seized:

H&W MODEL 1500 .308 RIFLE, 2 SCOPES, AR UPPER RECEIVER AND BARREL, PW ARMS SERIAL# 077832, 1 MAGAZINE (.308), 1 P&D SERIAL# G80239WC239 (32G), 1 P&D SN C5013WT3238 (16G), 512 MB SD CARD, 16B FLASH CARD, AR-15 PARTS (BAR, CHARGING HANDLE, BI-PID), 2 BOLTS, 4 GUN PARTS, AR-15 PARTS, 4 EMPTY AR-15 MAGAZINES, 72 PC. M&B JUMBO SILVER SALUTE, 12X FENCE, TIGER SCARING ROCKET, 24X M&B CRACKER WOLF PACK (x2), 20X CHINATOWN SHARP CRACKERS, 2000 WOLF PACK SUPER LOUD, 278 WOLF PACK SUPER LOUD BOTTLE ROCKET, BB PISTOL SIG SAVER P226 SERIAL# 31123183, KIMBER PRO COVERT II SERIAL# KR230819 45 CAL., 4 GLOCK MAGAZINES 9mm, 1 DAMAGED GLOCK MAGAZINE, 1 RIPLE PISTOL GRIP, RUBEN MKII .22LR PISTOL SCRAPEY OF SERIAL NUMBER, JENNING J-22 .22LR, 16 WINCHESTER 6.56 BULLETS, 3 MAGAZINES LOADED FOR KIMBER PRO COVERT II, AR-15 PARTS, MISCELLANEOUS AMMUNITION, MISCELLANEOUS AMMUNITION, MISCELLANEOUS AMMUNITION, HOME MADE SILENCER, MAGAZINE LOADED W/BBs, 3 MAGAZINES FOR RUBEN MKII .22LR AND BOX OF BULLETS, 29 RDS OF 45 CAL., 1 BOX OF 50 WINCHESTER 9mm BULLETS, 8MB COMPACT FLASH, 50 RDS OF 9mm AMMO, MISC AMMO, VICTORIA SECURE BOX WITH: CHARGING CORDS + ACCESSORIES, 4 MICRO SD CARDS, 9 PHOTOS.

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 8/25/2017

Executing officer's signature

JONATHAN A. BRANCH SPECIAL AGENT  
Printed name and title

**ATTACHMENT A**

**Property to Be Searched**

1. Storage locker B64 held under the name of Jeanine Ramadan located at Devon Self Storage Facility, 4750 S State St, Ann Arbor, Michigan. The locker has a blue door and the sign "B 64" is affixed next to the door.
2. The following items recovered from the person or luggage of Yousef Mohammad Ramadan at DTW airport:
  - a. ASUS Computer, Serial Number G4PDCG00111N
  - b. Hitachi Hard Drive, Serial Number JP1572JE0Y8AUK
  - c. Toshiba Laptop Computer, Serial Number 6E038858P
  - d. Lenovo Laptop Computer, Serial Number PF01AKSF
  - e. Ten (10) SD cards for a digital camera
  - f. Seagate Backup Plus external hard drive, Serial Number NA7TK85N
  - g. Seagate external hard drive, Serial Number 2GE7954V
  - h. Toshiba external hard drive, Serial Number X19JTA46TR48
  - i. Toshiba external hard drive, Serial Number 64PCTX7GT18B
  - j. Seagate external hard drive, Serial Number NA47PV822
  - k. One (1) DVD disc

- l. One (1) AT&T Sim Card
- m. One (1) San Disk Memory Stick-Pro Duo
- n. Apple iPhone 6, Model A1522, Serial Number F2LNT629G5QL
- o. Apple iPhone 6, Model A1524, Serial Number DTRSM0XJG5R2
- p. Apple iPhone 7, Model A1661, Serial Number F2LSR4XGHFY2
- q. Apple iPod, Model A1421, Serial Number CCQP47Y0G22Q

**ATTACHMENT B**

**Particular Things to be Seized**

All information that constitutes evidence of a violation of 18 U.S.C. §§ 842(a)(3)(A), 842(j), 26 U.S.C. § 5861(d), and 18 U.S.C. § 1001, involving Yousef Mohammad Ramadan, including, but not limited to, the following:

- a. Weapons, firearms, explosives, bombs, destructive devices, or hazardous materials;
- b. Items related to firearms, such as ammunition, holsters, sights, or grips;
- b. Items reasonably considered to constitute components of a destructive device or bomb, including, but not limited to: wiring, timers, shrapnel, or containers;
- c. Location information, including GPS data and content relating to locations used and frequented by the devices listed in Attachment A;
- d. All information relating to Yousef Mohammad Ramadan's motive for possessing explosives or firearms, including propaganda materials or other information related to ISIS, terrorism, or acts of terrorism.
- e. Information relating to Devon Self Storage Facility or any other person or entity that may be in possession of firearms, explosives, bombs or destructive devices on behalf of Yousef Mohammad Ramadan;

AO 106 (Rev. 04/10) Application for a Search Warrant      AUSA: Michael C. Martin      Telephone: (313) 226-9100  
 Special Agent: Ryan Y. Schanberger      Telephone: (313) 965-6088

# UNITED STATES DISTRICT COURT

for the  
 Eastern District of Michigan

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)

Devon Storage locker and various electronic devices more  
 fully described in Attachment A.

Case: 2:17-mc-51175 - 1  
 Case No. Judge: Borman, Paul D.  
 Filed: 08-23-2017  
 IN RE: SEALED MATTER (CMC)

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

I hereby certify that the foregoing is a certified copy of the original on file in this office.

Clerk, U.S. District Court  
 Eastern District of Michigan

By: s/Carolyn Ciesla  
 Deputy



The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 842(a)(3)(A)

Unlicensed receipt of explosive materials.

See attached AFFIDAVIT for more violations.

The application is based on these facts:

See attached AFFIDAVIT.

- ☒ Continued on the attached sheet.  
☒ Delayed notice 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Ryan Y. Schanberger  
 Applicant's signature

Ryan Y. Schanberger, Special Agent, FBI  
 Printed name and title

Sworn to before me and signed in my presence  
 and/or by reliable electronic means.

Date: 8/23/17

City and state: Detroit, MI

R. Steven Whalen  
 Judge's signature

R. Steven Whalen, U. S. Magistrate Judge  
 Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR EASTERN DISTRICT OF MICHIGAN  
SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF:

- a. ASUS Computer, Serial Number  
G4PDCG00111N
- b. Hitachi Hard Drive, Serial Number  
JP1572JE0Y8AUK
- c. Toshiba Laptop Computer, Serial Number  
6E038858P
- d. Lenovo Laptop Computer, Serial Number  
PF01AKSF
- e. Ten (10) SD cards for a digital camera
- f. Seagate Backup Plus external hard drive,  
Serial Number NA7TK85N
- g. Seagate external hard drive, Serial Number  
2GE7954V
- h. Toshiba external hard drive, Serial Number  
X19JTA46TR48
- i. Toshiba external hard drive, Serial Number  
64PCTX7GT18B
- j. Seagate external hard drive, Serial Number  
NA47PV822
- k. One (1) DVD disk
- l. One (1) AT&T Sim Card

Case No.

- m. One (1) San Disk Memory Stick-Pro Duo
- n. Apple iPhone 6, Model A1522, Serial Number F2LNT629G5QL
- o. Apple iPhone 6, Model A1524, Serial Number DTRSM0XJG5R2
- p. Apple iPhone 7, Model A1661, Serial Number F2LSR4XGHFY2
- q. Apple iPod, Model A1421, Serial Number CCQP47Y0G22Q
- r. Storage locker B64 held under the name of Jeanine Ramadan located at Devon Self Storage Facility, 4750 S State St, Ann Arbor, Michigan

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Ryan Y. Schanberger, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for the electronic devices and a storage locker further described in Attachment A that are associated with Yousef Mohammad Ramadan.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since November, 2012. I am currently assigned

to a counterterrorism squad in the FBI's Detroit Division. As part of my duties, I investigate criminal violations relating to terrorism. Since joining the FBI, I have conducted several investigations of suspected homegrown violent extremists who are believed to have been radicalized online by the global violent jihadist movement. My training and experience has given me a working knowledge of how terrorism suspects operate and of the indications that they may be mobilizing in order to commit acts of violence.

3. My knowledge of the facts and circumstances contained within this affidavit is based upon my personal investigation, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of the following offenses has occurred: 18 U.S.C. § 842(a)(3)(A), which prohibits the unlicensed receipt of explosive materials; 18 U.S.C. § 842(j), which prohibits the unlawful storage of explosives; and 26 U.S.C. § 5861(d), which prohibits the unlawful manufacturing, receipt, or possession of a destructive device (which is defined to include any explosive or bomb), and 18 U.S.C. § 1001 (which prohibits making false

statements). There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

### **PROBABLE CAUSE**

5. On August 15, 2017, Yousef Mohammad Ramadan, a 28 year old naturalized United States citizen, traveled to Detroit Metropolitan Wayne County (DTW) Airport with his wife and four minor children. Ramadan went to the ticket counter for Royal Jordanian Airlines and purchased six tickets for himself and the members of his family for a flight to Amman, Jordan that departed later that same day.

6. Prior to the departure of the flight, Transportation Security Administration officers discovered the following items in Ramadan's checked luggage: a rifle scope and mounts, knives, OC pepper spray, tactical load-bearing vests, a gas mask, a vest with ballistic plates, two-way radios, a taser weapon system with extra cartridges, a pistol holster, ammunition pouches, and black masks.

7. A secondary inspection revealed Ramadan was in possession of an Apple iPhone 7, Model A1661, Serial Number F2LSR4XGHFY2, on his person. Ramadan's wife, Jeanine Ramadan, had an Apple iPod, Model A1421, Serial Number CCQP47Y0G22Q, on her person. In addition, the following electronic devices were packed in Ramadan's checked luggage:

- a. ASUS Computer, Serial Number G4PDCG00111N;
- b. Hitachi Hard Drive, Serial Number JP1572JE0Y8AUK;
- c. Toshiba Laptop Computer, Serial Number 6E038858P;
- d. Lenovo Laptop Computer, Serial Number PF01AKSF;
- e. Ten (10) SD cards for a digital camera;
- f. Seagate Backup Plus external hard drive, Serial Number NA7TK85N;
- g. Seagate external hard drive, Serial Number 2GE7954V;
- h. Toshiba external hard drive, Serial Number X19JTA46TR48;
- i. Toshiba external hard drive, Serial Number 64PCTX7GT18B;
- j. Seagate external hard drive, Serial Number NA47PV822;
- k. One (1) DVD disc;
- l. One (1) AT&T Sim Card;
- m. One (1) San Disk Memory Stick-Pro Duo;
- n. Apple iPhone 6, Model A1522, Serial Number F2LNT629G5QL;
- o. Apple iPhone 6, Model A1524, Serial Number DTRSM0XJG5R2.

8. Officers from the United States Customs and Border Protection interviewed Ramadan. Ramadan told the CBP officers that he was leaving the United States to live in Palestine. When CBP officers asked Ramadan about the various items described above that were found in his luggage, Ramadan could not give an

answer and became very nervous. Due to Ramadan's inability to answer questions about the items, CBP officers examined the external media drives. On the external media drives were: (1) videos of Ramadan shooting pistols and rifles, including a sniper rifle; (2) photographs and videos of pipe bombs; and (3) propaganda videos and photographs related to the designated foreign terrorist organization The Islamic State of Iraq and al-Sham ("ISIS"), including videos of ISIS fighters wearing black masks similar to the black masks found in Ramadan's luggage.

9. On or about October 15, 2004, the United States Secretary of State designated al-Qaida in Iraq (AQI), then known as Jam 'at al Tawid wa' al-Jahid, as a Foreign Terrorist Organization (FTO) under Section 219 of the Immigration and Nationality Act, and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224. On or about May 15, 2014, the Secretary of State amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224 to add the alias "Islamic State of Iraq and the Levant" (ISIL) as its primary name. The Secretary of State also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham ("ISIS"—which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-'Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furquan Establishment for Media Production. On September 21, 2015, the Secretary

added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

10. FBI agents interviewed Ramadan later on August 15, 2017. FBI agents presented Ramadan with a photograph obtained from his electronic media which depicted what appeared to be glass on a colored floor tile or counter-top tile. Ramadan stated that the items in the picture were broken glass pieces piled up on the tiled floor at his residence in Israel. He was then shown a picture of what appeared to be a homemade IED, also taken from review of his electronic media, that appeared to be made of a metal elbow joint, capped at both ends, with a fuse extending out of it. This type of device is often referred to as a pipe bomb. When asked about this, Ramadan stated that it was like a large firework that would make a loud bang when detonated, and that these items were sometimes used to throw at soldiers overseas. Interviewing agents then advised that the IED appeared to be photographed on the same flooring as the glass shard he admitted to be on the floor of his residence, to which Ramadan responded that all floor tiles overseas are similar in appearance and that he had in fact downloaded this image from the Internet. Ramadan was then asked specifically how long it took him to construct that pictured device and without hesitation he stated about one hour. Ramadan then immediately recanted, stating that he meant it would take about one hour if he had

had all the components needed to make the device. Ramadan was also asked what was used as shrapnel in the device and he responded that “they” put bullets inside.

11. Ramadan stated that he had made explosive devices before for “educational purposes” while overseas and had tested one by throwing it against a wall. He described the device as cylindrical in shape, approximately 2” long and similar to a CO2 cartridge, with a wick.

12. Ramadan acknowledged that the tactical items found in his checked luggage all belonged to him and claimed to have purchased them for personal protection, outdoor use, and for making his YouTube videos. Ramadan stated that he made several videos for his YouTube channels, which include a channel entitled “WB.88Guns.” I have examined the YouTube channel entitled “WB.88Guns.” This channel contains seven videos, which were posted between November 12, 2016, and February 23, 2017. The videos show an individual shooting or handling various types of firearms, including a Glock pistol, a Kimber Pro Covert pistol, a Winchester shotgun and a Mosin Nagant sniper rifle.

13. The video pertaining to the Kimber Pro Covert pistol was posted on December 1, 2016. Text containing a description of the video was posted at the same time as the video. The text states, in part, “SO HERE IS A NICE VIDEO SHOWING MY KIMBER PRO COVERT II (45 ACP).” Records from the State of Michigan

show that a Kimber 45 caliber Covert II pistol, serial number KR230819, is currently registered to Ramadan. The descriptive text from the Kimber Pro Covert YouTube video also states that the firearm "HAS A DESERT DIGITAL CAMO GRIP." Of the seven videos posted to "WB.88Guns," five of them take place outdoors in arid environments. The remaining two videos take place indoors.

14. During the interview with FBI agents, Ramadan stated that he currently owns three weapons, including two rifles and a Glock pistol that he placed in a self-storage location before departing for the airport. Ramadan did not disclose that he also owns the Kimber Pro Covert pistol. However, Ramadan immediately recanted and stated that he left the three firearms with a friend whose identity he would not provide.

15. On August 17, 2017, FBI made contact with a representative at the Devon Self Storage facility, located at 4750 S State St, Ann Arbor, Michigan. According to business records from Devon Self Storage, there is a storage locker there in the name of Jeanine Ramadan, Yousef Ramadan's wife. Records from Devon Self Storage facility show that: (1) Jeanine Ramadan rents a storage locker, unit B64, there on a month-to-month basis; (2) rent was paid for that storage locker on or about August 7, 2017, for the period ending on August 31, 2017; (3) "Mohammad Ramadan" is listed as an emergency contact on the "new customer

information sheet” completed by Jeanine Ramadan; (4) the storage locker was accessed on August 15, 2017, from 11:03 to 11:05 a.m.. FBI agents reviewed security camera video at the Devon Self Storage facility for this time period and observed that a male driving a Honda Odyssey minivan accessed the storage facility during this time period. A Honda Odyssey minivan is registered to Somaya Abufarha, at 4604 Nutmeg, Ypsilanti, Michigan. Somaya Abufarha is Ramadan’s sister. On August 15, 2017, Ramadan and his family were unable to make the flight to Amman, Jordan, on time. Ramadan’s wife, Jeanine Ramadan, told FBI agents on August 15, 2017, that she (Jeanine Ramadan) and Ramadan would reside with Ramadan’s sister at 4604 Nutmeg, Ypsilanti, Michigan. Since August 15, 2017, FBI agents conducted surveillance at 4604 Nutmeg, Ypsilanti, Michigan, and observed Ramadan at the residence on several occasions. In addition, Immigration and Customs Enforcement agents examined the Apple iPhone 7, Model A1661, Serial Number F2LSR4XGHFY2, that Ramadan had on his person at the airport on August 15, 2017, and found a copy of a letter from Devon Self Storage regarding the payment of rent for August, 2017.

16. During the same interview, Ramadan was questioned regarding the ISIS propaganda videos and photographs on his electronic media. Ramadan stated that he likes and watches all aspects of combat footage. He claimed that he does

support ISIS' goal of establishing the Caliphate and an Islamic State, but that he does not support their methods of violence to achieve that goal, instead preferring a peaceful approach to converting non-believers into the Muslim religion and/or forming an Islamic State.

17. When advised that viewing violent ISIS videos could lead to violence on his part, Ramadan responded by saying that if he ever wanted to commit an attack he certainly would not have to travel overseas to do it. Ramadan stated that he would do it in the United States as it would be much easier to accomplish than overseas. Ramadan stated that even if his weapons were confiscated, he could simply buy more weapons off the street to utilize, and that an attack in the United States would be far easier than attempting to do something overseas. Ramadan further stated that a domestic attack would still be viewed and praised as a huge victory by ISIS. Ramadan explained that he would never conduct any type of attack overseas because the Israelis retaliate against every family member for the acts of the perpetrator, even though they had no involvement.

18. Ramadan also told the FBI agents that he is a very private person and that he does not trust anyone, including his wife. Ramadan stated that he does not know if she will use something against him, as she has done in the past. Ramadan

further stated that he is a loner and that he keeps to himself because he does not trust anyone.

19. On August 17, 2017, the Bureau of Alcohol, Tobacco, Firearms and Explosives reported to the FBI that there exists no license on record for Ramadan to possess explosive material.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. The Device has the capability to access the internet. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

22. Data on the storage medium can provide evidence of a file that was

once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- a. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore,

contextual information necessary to understand other evidence also falls within the scope of the warrant.

23. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

#### **CONCLUSION AS TO PROBABLE CAUSE**

26. Given the evidence set forth above, your affiant submits that there is probable cause to believe that a violation of the following offenses has occurred: 18

U.S.C. § 842(a)(3)(A), which prohibits the unlicensed receipt of explosive materials; 18 U.S.C. § 842(j), which prohibits the unlawful storage of explosives; and 26 U.S.C. § 5861(d), which prohibits the unlawful manufacturing, receipt, or possession of a destructive device (which is defined to include any explosive or bomb), and 18 U.S.C. § 1001 (which prohibits making false statements). There is also probable cause to believe that evidence of these crimes, as further described in Attachment B, will be found in the electronic devices and storage locker further described in Attachment A.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

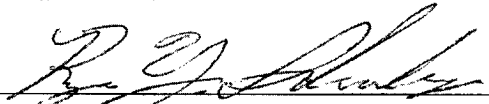
27. I anticipate executing this warrant on the devices described in Attachment A, which are currently in the possession of the Department of Homeland Security. Upon receipt of the information described in Attachment A, government-authorized persons will review that information to locate the items described in Attachment B.

#### **REQUEST FOR SEALING**

28. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into a terrorist

organization. Based upon my training and experience, I have learned that, terrorists and criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

  
\_\_\_\_\_  
RYAN Y. SCHANBERGER  
Special Agent  
Federal Bureau of Investigation

Sword to before me and signed in my  
Presence and/or by reliable electronic means..



8/23/17

\_\_\_\_\_  
HON. R. STEVEN WHALEN  
EXECUTIVE UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

1. Storage locker B64 held under the name of Jeanine Ramadan located at Devon Self Storage Facility, 4750 S State St, Ann Arbor, Michigan. The locker has a blue door and the sign "B 64" is affixed next to the door.
2. The following items recovered from the person or luggage of Yousef Mohammad Ramadan at DTW airport:
  - a. ASUS Computer, Serial Number G4PDCG00111N
  - b. Hitachi Hard Drive, Serial Number JP1572JE0Y8AUK
  - c. Toshiba Laptop Computer, Serial Number 6E038858P
  - d. Lenovo Laptop Computer, Serial Number PF01AKSF
  - e. Ten (10) SD cards for a digital camera
  - f. Seagate Backup Plus external hard drive, Serial Number NA7TK85N
  - g. Seagate external hard drive, Serial Number 2GE7954V
  - h. Toshiba external hard drive, Serial Number X19JTA46TR48
  - i. Toshiba external hard drive, Serial Number 64PCTX7GT18B
  - j. Seagate external hard drive, Serial Number NA47PV822
  - k. One (1) DVD disc

- l. One (1) AT&T Sim Card
- m. One (1) San Disk Memory Stick-Pro Duo
- n. Apple iPhone 6, Model A1522, Serial Number F2LNT629G5QL
- o. Apple iPhone 6, Model A1524, Serial Number DTRSM0XJG5R2
- p. Apple iPhone 7, Model A1661, Serial Number F2LSR4XGHFY2
- q. Apple iPod, Model A1421, Serial Number CCQP47Y0G22Q

**ATTACHMENT B**

**Particular Things to be Seized**

All information that constitutes evidence of a violation of 18 U.S.C. §§ 842(a)(3)(A), 842(j), 26 U.S.C. § 5861(d), and 18 U.S.C. § 1001, involving Yousef Mohammad Ramadan, including, but not limited to, the following:

- a. Weapons, firearms, explosives, bombs, destructive devices, or hazardous materials;
- b. Items related to firearms, such as ammunition, holsters, sights, or grips;
- b. Items reasonably considered to constitute components of a destructive device or bomb, including, but not limited to: wiring, timers, shrapnel, or containers;
- c. Location information, including GPS data and content relating to locations used and frequented by the devices listed in Attachment A;
- d. All information relating to Yousef Mohammad Ramadan's motive for possessing explosives or firearms, including propaganda materials or other information related to ISIS, terrorism, or acts of terrorism.
- e. Information relating to Devon Self Storage Facility or any other person or entity that may be in possession of firearms, explosives, bombs or destructive devices on behalf of Yousef Mohammad Ramadan;

f. Information relating to who used, accessed, possessed or communicated with the items listed in Attachment A.

The term “information,” includes information in all forms, including paper, photographic, video, or any other type of electronic coding or data.

## UNITED STATES DISTRICT COURT

for the  
Eastern District of MichiganIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Devon Storage locker and various electronic devices more  
fully described in Attachment A.Case No. Case: 2:17-mc-51175 - 1  
Judge: Borman, Paul D.

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer.

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Eastern District of Michigan.  
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A..

I hereby certify that the foregoing is a certified copy  
of the original on file in this office.Clerk, U.S. District Court  
Eastern District of MichiganBy: s/Carolyn Ciesla  
DeputyI find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B.

**YOU ARE COMMANDED** to execute this warrant on or before September 6, 2017 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.  
(United States Magistrate Judge)☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☒ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_Date and time issued: 8/23/17 1:27 pmCity and state: Detroit, MI

Judge's signature

R. Steven Whalen, U. S. Magistrate Judge  
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

**ATTACHMENT A**

**Property to Be Searched**

1. Storage locker B64 held under the name of Jeanine Ramadan located at Devon Self Storage Facility, 4750 S State St, Ann Arbor, Michigan. The locker has a blue door and the sign "B 64" is affixed next to the door.
  
2. The following items recovered from the person or luggage of Yousef Mohammad Ramadan at DTW airport:
  - a. ASUS Computer, Serial Number G4PDCG00111N
  - b. Hitachi Hard Drive, Serial Number JP1572JE0Y8AUK
  - c. Toshiba Laptop Computer, Serial Number 6E038858P
  - d. Lenovo Laptop Computer, Serial Number PF01AKSF
  - e. Ten (10) SD cards for a digital camera
  - f. Seagate Backup Plus external hard drive, Serial Number NA7TK85N
  - g. Seagate external hard drive, Serial Number 2GE7954V
  - h. Toshiba external hard drive, Serial Number X19JTA46TR48
  - i. Toshiba external hard drive, Serial Number 64PCTX7GT18B
  - j. Seagate external hard drive, Serial Number NA47PV822
  - k. One (1) DVD disc

- l. One (1) AT&T Sim Card
- m. One (1) San Disk Memory Stick-Pro Duo
- n. Apple iPhone 6, Model A1522, Serial Number F2LNT629G5QL
- o. Apple iPhone 6, Model A1524, Serial Number DTRSM0XJG5R2
- p. Apple iPhone 7, Model A1661, Serial Number F2LSR4XGHFY2
- q. Apple iPod, Model A1421, Serial Number CCQP47Y0G22Q

**ATTACHMENT B**

**Particular Things to be Seized**

All information that constitutes evidence of a violation of 18 U.S.C. §§ 842(a)(3)(A), 842(j), 26 U.S.C. § 5861(d), and 18 U.S.C. § 1001, involving Yousef Mohammad Ramadan, including, but not limited to, the following:

- a. Weapons, firearms, explosives, bombs, destructive devices, or hazardous materials;
- b. Items related to firearms, such as ammunition, holsters, sights, or grips;
- b. Items reasonably considered to constitute components of a destructive device or bomb, including, but not limited to: wiring, timers, shrapnel, or containers;
- c. Location information, including GPS data and content relating to locations used and frequented by the devices listed in Attachment A;
- d. All information relating to Yousef Mohammad Ramadan's motive for possessing explosives or firearms, including propaganda materials or other information related to ISIS, terrorism, or acts of terrorism.
- e. Information relating to Devon Self Storage Facility or any other person or entity that may be in possession of firearms, explosives, bombs or destructive devices on behalf of Yousef Mohammad Ramadan;

f. Information relating to who used, accessed, possessed or communicated with the items listed in Attachment A.

The term “information,” includes information in all forms, including paper, photographic, video, or any other type of electronic coding or data.

# EXHIBIT B

iPhone 8

Overview

iOS

Tech Specs

Buy

iPhone 8

iPhone 8 Plus

Finish

Gold, Silver, Space Gray

Gold, Silver, Space Gray

Capacity<sup>1</sup>

64GB  
256GB

64GB  
256GB

Size and Weight<sup>2</sup>

5.45 inches  
(138.4 mm)

2.65 inches  
(67.3 mm)

6.24 inches  
(158.4 mm)

3.07 inches  
(78.1 mm)

0.29 inch  
(7.3 mm)

0.30 inch  
(7.5 mm)

Weight: 5.22 ounces (148 grams)

Weight: 7.13 ounces (202 grams)

Display

Retina HD display	Retina HD display
4.7-inch (diagonal) widescreen LCD Multi-Touch display with IPS technology	5.5-inch (diagonal) widescreen LCD Multi-Touch display with IPS technology
1334-by-750-pixel resolution at 326 ppi	1920-by-1080-pixel resolution at 401 ppi
1400:1 contrast ratio (typical)	1300:1 contrast ratio (typical)

- Both models:**
- True Tone display
  - Wide color display (P3)
  - 3D Touch
  - 625 cd/m2 max brightness (typical)
  - Dual-domain pixels for wide viewing angles
  - Fingerprint-resistant oleophobic coating
  - Support for display of multiple languages and characters simultaneously
  - Display Zoom
  - Reachability

<b>Splash, Water, and Dust Resistant<sup>3</sup></b>	Rated IP67 under IEC standard 60529
------------------------------------------------------	-------------------------------------

Chip

- A11 Bionic chip with 64-bit architecture
- Neural engine
- Embedded M11 motion coprocessor

<b>Camera</b>	12MP camera f/1.8 aperture	12MP wide-angle and telephoto cameras
---------------	-------------------------------	---------------------------------------

Wide-angle:  $f/1.8$  aperture

Telephoto:  $f/2.8$  aperture

Digital zoom up to 5x

—

—

Optical zoom; digital zoom up to 10x

Portrait mode

Portrait Lighting (beta)

#### Both models:

Optical image stabilization

Six-element lens

Quad-LED True Tone flash with Slow Sync

Panorama (up to 63MP)

Sapphire crystal lens cover

Backside illumination sensor

Hybrid IR filter

Autofocus with Focus Pixels

Tap to focus with Focus Pixels

Live Photos with stabilization

Wide color capture for photos and Live Photos

Improved local tone mapping

Body and face detection

Exposure control

Noise reduction

Auto HDR for photos

Auto image stabilization

Burst mode

Timer mode

Photo geotagging

Image formats captured: HEIF and JPEG

---

## Video Recording

4K video recording at 24 fps, 30 fps, or 60 fps

1080p HD video recording at 30 fps or 60 fps

720p HD video recording at 30 fps

Optical image stabilization for video

Optical zoom; 6x digital zoom (iPhone 8 Plus only)

Quad-LED True Tone flash

Slo-mo video support for 1080p at 120 fps or 240 fps

Time-lapse video with stabilization

Cinematic video stabilization (1080p and 720p)

Continuous autofocus video

- Body and face detection
- Noise reduction
- Take 8MP still photos while recording 4K video
- Playback zoom
- Video geotagging
- Video formats recorded: HEVC and H.264

---

**FaceTime HD Camera**

- 7MP camera
- 1080p HD video recording
- Retina Flash
- f*/2.2 aperture
- Wide color capture for photos and Live Photos
- Auto HDR
- Backside illumination sensor
- Body and face detection
- Auto image stabilization
- Burst mode
- Exposure control
- Timer mode

---

**Touch ID**

Fingerprint sensor built into the Home button

---

**Apple Pay**

- Pay with your iPhone using Touch ID in stores, within apps, and on the web
- Complete purchases made with Apple Pay on your Mac
- Receive and redeem rewards using rewards cards
- Learn more about Apple Pay ›

---

**Carriers**

---

Cellular and Wireless	Model A1863*	FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 29, 30, 66)
	Model A1864*	TD-LTE (Bands 34, 38, 39, 40, 41)
		TD-SCDMA 1900 (F), 2000 (A)
		CDMA EV-DO Rev. A (800, 1900, 2100 MHz)
		UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
		GSM/EDGE (850, 900, 1800, 1900 MHz)
	Model A1905*	FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 29, 30, 66)
	Model A1897*	TD-LTE (Bands 34, 38, 39, 40, 41)
		UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
		GSM/EDGE (850, 900, 1800, 1900 MHz)
	All models	802.11ac Wi-Fi with MIMO
		Bluetooth 5.0 wireless technology
		NFC with reader mode

Location	Assisted GPS, GLONASS, Galileo, and QZSS
	Digital compass
	Wi-Fi
	Cellular
	iBeacon microlocation

Video Calling <sup>4</sup>	FaceTime video calling over Wi-Fi or cellular
----------------------------	-----------------------------------------------

Audio Calling <sup>4</sup>	FaceTime audio
	Voice over LTE (VoLTE) <sup>5</sup>
	Wi-Fi calling <sup>5</sup>

Audio Playback	Audio formats supported: AAC-LC, HE-AAC, HE-AAC v2, Protected AAC, MP3, Linear PCM, Apple Lossless, FLAC, Dolby Digital (AC-3), Dolby Digital Plus (E-AC-3), and Audible (formats 2, 3, 4, Audible Enhanced Audio, AAX, and AAX+)
	User-configurable maximum volume limit

Video Playback

Video formats supported: HEVC, H.264, MPEG-4 Part 2, and Motion JPEG

Supports Dolby Vision and HDR10 content

AirPlay Mirroring, photos, and video out to Apple TV (2nd generation or later)<sup>6</sup>

Video mirroring and video out support: Up to 1080p through Lightning Digital AV Adapter and Lightning to VGA Adapter (adapters sold separately)<sup>6</sup>

Siri<sup>7</sup>

Use your voice to send messages, set reminders, and more

Get intelligent suggestions in Messages, Mail, QuickType, and more

Activate with only your voice using “Hey Siri”

Listen and identify songs

Learn more about Siri >

External Buttons and Connectors

Home/Touch ID sensor

Volume up/down Ring/Silent switch

Lightning connector

Side button

Built-in stereo speaker  
Built-in microphone

Built-in microphone

Built-in stereo speaker

## Power and Battery<sup>8</sup>

Lasts about the same as iPhone 7

Lasts about the same as iPhone 7 Plus

### Talk time (wireless):

Up to 14 hours

### Talk time (wireless):

Up to 21 hours

### Internet use:

Up to 12 hours

### Internet use:

Up to 13 hours

### Video playback (wireless):

Up to 13 hours

### Video playback (wireless):

Up to 14 hours

### Audio playback (wireless):

Up to 40 hours

### Audio playback (wireless):

Up to 60 hours

### Fast-charge capable:

Up to 50% charge 30 minutes<sup>9</sup>

### Fast-charge capable:

Up to 50% charge 30 minutes<sup>9</sup>

### Both models:

Built-in rechargeable lithium-ion battery

Wireless charging (works with Qi chargers<sup>10</sup>)

Charging via USB to computer system or power adapter

## Sensors

Touch ID fingerprint sensor

Barometer

Three-axis gyro

Accelerometer

Proximity sensor

Ambient light sensor

## Operating System

### iOS 11

With new features and capabilities that let you get more done quickly and easily, iOS 11 makes iPhone more powerful, personal, and intelligent than ever.

[See what's new in iOS 11 >](#)

## Accessibility

Accessibility features help people with disabilities get the most out of their new iPhone 8. With built-in support for vision, hearing, physical and motor skills, and learning and literacy, you can fully enjoy the world's most personal device. [Learn more >](#)

Features include:

- VoiceOver
  - Zoom
  - Magnifier
  - Software TTY
- Siri and Dictation
  - Type to Siri
  - Switch Control
  - Closed Captions
- AssistiveTouch
  - Speak Screen

Built-in Apps

Camera	Photos	Health	Messages	Phone	FaceTime
Mail	Music	Wallet	Safari	Maps	Siri
Calendar	iTunes Store	App Store	Notes	News	Contacts
iBooks	Home	Weather	Reminders	Clock	TV
Stocks	Calculator	Voice Memos	Compass	Podcasts	Watch
Tips	Find My iPhone	Find My Friends	Settings	Files	

Free Apps from Apple<sup>11</sup>

Pages, Numbers, Keynote, iMovie, GarageBand, iTunes U, and Clips are preinstalled.

iMovie	Pages	Numbers	Keynote	iTunes U	GarageBand
Apple Store	Trailers	Apple TV Remote	iTunes Remote	Music Memos	Clips

Headphones

EarPods with Lightning Connector

---

## SIM Card

Nano-SIM

iPhone 8 and iPhone 8 Plus are not compatible with existing micro-SIM cards.

---

## Rating for Hearing Aids

iPhone 8 (Model A1863, A1905): M3, T4

iPhone 8 Plus (Model A1864, A1897): M3, T4

---

## Mail Attachment Support

### Viewable document types

.jpg, .tiff, .gif (images); .doc and .docx (Microsoft Word); .htm and .html (web pages); .key (Keynote); .numbers (Numbers); .pages (Pages); .pdf (Preview and Adobe Acrobat); .ppt and .pptx (Microsoft PowerPoint); .txt (text); .rtf (rich text format); .vcf (contact information); .xls and .xlsx (Microsoft Excel); .zip; .ics

---

## System Requirements

Apple ID (required for some features)

Internet access<sup>12</sup>

Syncing with iTunes on a Mac or PC requires:

- **Mac:** OS X 10.10.5 or later
  - **PC:** Windows 7 or later
  - iTunes 12.7 or later (free download from [www.itunes.com/download](http://www.itunes.com/download))
- 

## Environmental Requirements

**Operating ambient temperature:** 32° to 95° F (0° to 35° C)

**Nonoperating temperature:** -4° to 113° F (-20° to 45° C)

**Relative humidity:** 5% to 95% noncondensing

**Operating altitude:** tested up to 10,000 feet (3000 m)

---

## Languages

### Language support

English (Australia, UK, U.S.), Chinese (Simplified, Traditional, Traditional Hong Kong), French (Canada, France), German, Italian, Japanese, Korean, Spanish (Latin America, Mexico, Spain), Arabic, Catalan, Croatian, Czech, Danish, Dutch, Finnish, Greek, Hebrew, Hindi, Hungarian,

Indonesian, Malay, Norwegian, Polish, Portuguese (Brazil, Portugal), Romanian, Russian, Slovak, Swedish, Thai, Turkish, Ukrainian, Vietnamese

**QuickType keyboard support**

English (Australia, Canada, India, Singapore, UK, U.S.), Chinese - Simplified (Handwriting, Pinyin, Stroke), Chinese - Traditional (Cangjie, Handwriting, Pinyin, Stroke, Sucheng, Zhuyin), French (Belgium, Canada, France, Switzerland), German (Austria, Germany, Switzerland), Italian, Japanese (Kana, Romaji), Korean, Spanish (Latin America, Mexico, Spain), Arabic (Modern Standard, Najdi), Armenian, Azerbaijani, Belarusian, Bengali, Bulgarian, Catalan, Cherokee, Croatian, Czech, Danish, Dutch, Emoji, Estonian, Filipino, Finnish, Flemish, Georgian, Greek, Gujarati, Hawaiian, Hebrew, Hindi (Devanagari, Transliteration), Hinglish, Hungarian, Icelandic, Indonesian, Irish, Kannada, Latvian, Lithuanian, Macedonian, Malay, Malayalam, Maori, Marathi, Norwegian, Odia, Persian, Polish, Portuguese (Brazil, Portugal), Punjabi, Romanian, Russian, Serbian (Cyrillic, Latin), Slovak, Slovenian, Swahili, Swedish, Tamil (Script, Transliteration), Telugu, Thai, Tibetan, Turkish, Ukrainian, Urdu, Vietnamese, Welsh

**QuickType keyboard support with predictive input**

English (Australia, Canada, India, Singapore, UK, U.S.), Chinese (Simplified, Traditional), French (Belgium, Canada, France, Switzerland), German (Austria, Germany, Switzerland), Italian, Japanese, Korean, Russian, Spanish (Latin America, Mexico, Spain), Portuguese (Brazil, Portugal), Thai, Turkish

**Siri languages**

English (Australia, Canada, India, Ireland, New Zealand, Singapore, South Africa, UK, U.S.), Spanish (Chile, Mexico, Spain, U.S.), French (Belgium, Canada, France, Switzerland), German (Austria, Germany, Switzerland), Italian (Italy, Switzerland), Japanese, Korean, Mandarin (Mainland China, Taiwan), Cantonese (Mainland China, Hong Kong, Macao), Arabic (Saudi Arabia, United Arab Emirates), Danish (Denmark), Dutch (Belgium, Netherlands), Finnish (Finland), Hebrew (Israel), Malay (Malaysia), Norwegian (Norway), Portuguese (Brazil), Russian (Russia), Swedish (Sweden), Thai (Thailand), Turkish (Turkey)

**Dictation languages**

English (Australia, Canada, India, Indonesia, Ireland, Malaysia, New Zealand, Philippines, Saudi Arabia, Singapore, South Africa, United Arab Emirates, UK, U.S.), Spanish (Argentina, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Panama, Paraguay, Peru, Spain, Uruguay, U.S.), French (Belgium, Canada, France, Luxembourg, Switzerland), German (Austria, Germany, Luxembourg, Switzerland), Italian (Italy, Switzerland), Japanese, Korean, Mandarin (Mainland China, Taiwan), Cantonese (Mainland China, Hong Kong, Macao), Arabic (Kuwait, Qatar, Saudi Arabia, United Arab Emirates), Catalan, Croatian, Czech, Danish, Dutch (Belgium, Netherlands), Finnish, Greek, Hebrew, Hindi (India), Hungarian, Indonesian, Malaysian, Norwegian, Polish, Portuguese (Brazil, Portugal), Romanian, Russian, Shanghaiese (Mainland China), Slovakian, Swedish, Thai, Turkish, Ukrainian, Vietnamese

**Definition dictionary support**

English, Chinese (Simplified, Traditional), Danish, Dutch, French, German, Hindi, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Thai, Turkish

**Bilingual dictionary support**

Chinese (Simplified), Dutch, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish

**Spell check**

English, French, German, Italian, Spanish, Danish, Dutch, Finnish, Korean, Norwegian, Polish, Portuguese, Russian, Swedish, Turkish

## In the Box

iPhone with iOS 11  
EarPods with Lightning Connector  
Lightning to 3.5 mm Headphone Jack Adapter  
Lightning to USB Cable  
USB Power Adapter  
Documentation

## iPhone and the Environment

Apple takes a complete product life cycle approach to determining our environmental impact. [Learn more >](#)

**iPhone 8 and iPhone 8 Plus embody Apple's continuing environmental progress. They are designed with the following features to reduce environmental impact:**

- Mercury-free LED-backlit display
- Arsenic-free display glass
- Brominated flame retardant-free
- PVC-free
- Beryllium-free
- Highly recyclable aluminum

### Apple and the Environment

Learn more about Apple's dedication to reducing the environmental impact of our products and process. Or read our **Product Environmental Reports** for detailed information on the environmental performance of every Apple product.

### Recycling

Apple takes a holistic view of materials management and waste minimization. [Learn more about how to recycle your iPhone >](#)

**iPhone X  
Tech Specs**[Learn more ›](#)**iPhone 7  
Tech Specs**[Learn more ›](#)**iPhone 6s  
Tech Specs**[Learn more ›](#)**iPhone SE  
Tech Specs**[Learn more ›](#)

## Compare iPhone models

[Find the best iPhone for you ›](#)

The easiest way to upgrade  
to the latest iPhone.\*\*

[Learn more >](#)

Get up to \$375 in credit toward the  
purchase of iPhone 8 when you trade in  
your eligible smartphone.†

[Learn more >](#)

Free two-day delivery

On in-stock items ordered by  
5:00 p.m.

[Learn more >](#)

Apple Store app

The easiest way to buy your new  
iPhone, right from your current  
iPhone.

[Download now >](#)

Special financing

Apply for special financing and  
earn rewards.

[Learn more >](#)

Get help buying

Have a question? Call a  
Specialist or chat online.  
Call 1-800-MY-APPLE.

[Chat now >](#)

\* To identify your iPhone model number, see <http://support.apple.com/kb/HT3939>. For details on LTE support, contact your carrier and see [www.apple.com/iphone/LTE](http://www.apple.com/iphone/LTE). Cellular technology support is based on iPhone model number and configuration for either CDMA or GSM networks.

- 1. Available space is less and varies due to many factors. A standard configuration uses approximately 8GB to 11GB of space (including iOS and preinstalled apps) depending on the model and settings. Preinstalled apps use about 4GB, and you can delete these apps and restore them.
  - 2. Size and weight vary by configuration and manufacturing process.
  - 3. iPhone 8 and iPhone 8 Plus are splash, water, and dust resistant and were tested under controlled laboratory conditions with a rating of IP67 under IEC standard 60529. Splash, water, and dust resistance are not permanent conditions and resistance might decrease as a result of normal wear. Do not attempt to charge a wet iPhone; refer to the user guide for cleaning and drying instructions. Liquid damage not covered under warranty.
  - 4. FaceTime calling requires a FaceTime-enabled device for the caller and recipient and a Wi-Fi connection. Availability over a cellular network depends on carrier policies; data charges may apply.
  - 5. Data plan required. LTE Advanced, LTE, VoLTE, and Wi-Fi calling are available in select markets and through select carriers. Speeds are based on theoretical throughput and vary based on site conditions and carrier. For details on LTE support, contact your carrier and see [www.apple.com/iphone/LTE](http://www.apple.com/iphone/LTE).
  - 6. Standard Dynamic Range video content only.
  - 7. Siri may not be available in all languages or in all areas, and features may vary by area. Internet access required. Cellular data charges may apply.
  - 8. All battery claims depend on network configuration and many other factors; actual results will vary. Battery has limited recharge cycles and may eventually need to be replaced by Apple service provider. Battery life and charge cycles vary by use and settings. See [www.apple.com/batteries](http://www.apple.com/batteries) and [www.apple.com/iphone/battery.html](http://www.apple.com/iphone/battery.html) for more information.
  - 9. Testing conducted by Apple in August 2017 using preproduction iPhone 8 and iPhone 8 Plus units and software and accessory Apple USB-C Power Adapters (29W Model A1540, 61W Model A1718, 87W Model A1719). Fast-charge testing conducted with drained iPhone units. Charge time varies with environmental factors; actual results will vary.
  - 10. Compatible wireless charging mats sold separately.
  - 11. iMovie, GarageBand, Pages, Numbers, and Keynote are available on the App Store. Downloading apps requires an Apple ID and a device that is compatible with the iOS version required for each app.
  - 12. Wireless broadband recommended; fees may apply.
- Some features may not be available for all countries or all areas. [Click here](#) to see complete list.

\*\* The iPhone Upgrade Program is available to qualified customers and requires service with AT&T, Sprint, T-Mobile, or Verizon. A two-year installment loan and iPhone activation are required. Terms apply.

† Trade-in values may vary based on the condition and model of your smartphone trade-in. Offer may not be available in all stores and not all devices are eligible for credit. Additional terms apply. [Learn more.](#)

iPhone	iPhone 8	Tech Specs		
<b>Shop and Learn</b>		<b>Apple Store</b>	<b>For Education</b>	<b>Account</b>
Mac		Find a Store	Apple and Education	Manage Your Apple ID
iPad		Genius Bar	Shop for College	Apple Store Account
iPhone		Today at Apple		iCloud.com
Watch		Apple Camp	<b>For Business</b>	
TV		Field Trip	Apple and Business	<b>Apple Values</b>
Music		Apple Store App	Shop for Business	Accessibility
iTunes		Refurbished and Clearance		Education
				Environment
				<b>About Apple</b>
				Newsroom
				Apple Leadership
				Job Opportunities
				Investors
				Events
				Contact Apple

- HomePod
- Financing
- Inclusion and Diversity
- iPod touch
- Reuse and Recycling
- Privacy
- Accessories
- Order Status
- Supplier Responsibility
- Gift Cards
- Shopping Help

More ways to shop: Visit an [Apple Store](#), call 1-800-MY-APPLE, or [find a reseller](#).

# EXHIBIT C



# PewResearchCenter

*Internet, Science & Tech*

MENU

RESEARCH AREAS

FACT SHEET

JANUARY 12, 2017

## Mobile Fact Sheet

MORE FACT SHEETS: [INTERNET/BROADBAND](#) | [SOCIAL MEDIA](#)

Mobile phone ownership  
over time

Who owns cellphones  
and smartphones

Ownership of other  
devices

Smartphone  
dependency over time

Who is smartphone  
dependent

Find out more

largely stationary internet of the early 2000s, Americans today are increasingly connected to the information while “on the go” via smartphones and other mobile devices. Explore the patterns and shaped the mobile revolution below.



### Mobile phone ownership over time

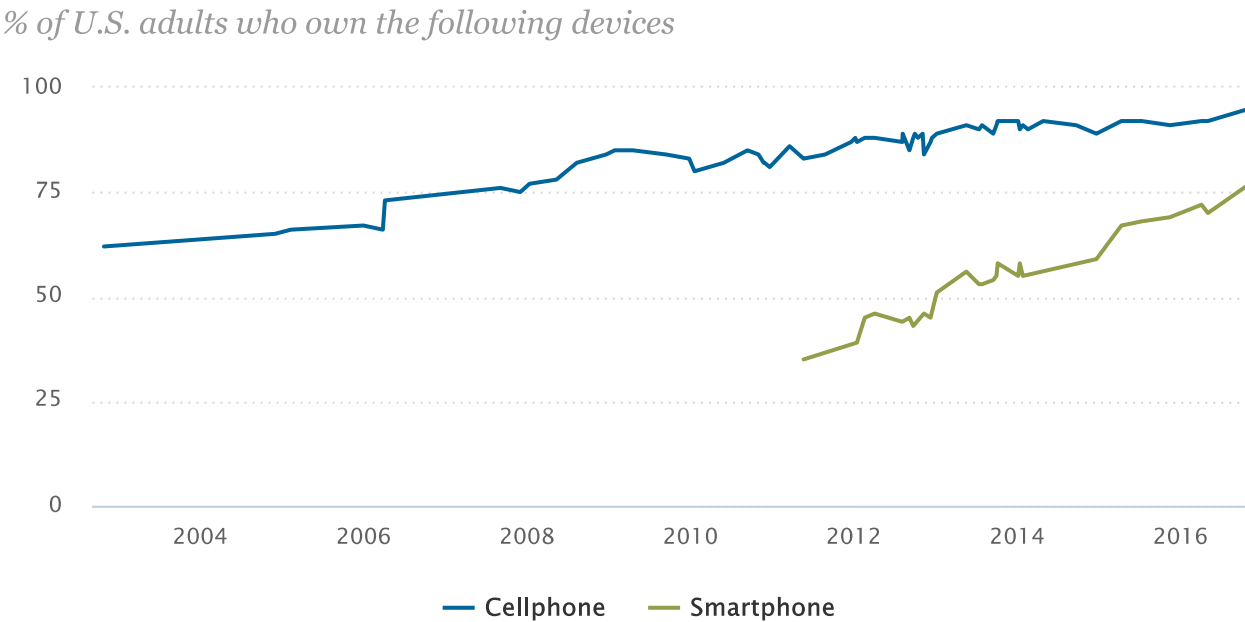
of Americans – 95% – now own a cellphone of some kind. The share of Americans that own smartphones is now 77%, up from just 35% in Pew Research Center’s first survey of smartphone ownership conducted in 2011.

Chart

Data

Share

Embed



Source: Surveys conducted 2002-2016.

PEW RESEARCH CENTER



Who owns cellphones and smartphones

A substantial majority of Americans are cellphone owners across a wide range of demographic groups. By contrast, smartphone ownership exhibits greater variation based on age, household income and educational attainment.

*% of U.S. adults who own the following devices*

	Any cellphone	Smartphone	Cellphone, but not smartphone
Total	95%	77%	18%
Men	96%	78%	18%
Women	94%	75%	19%
White	94%	77%	17%

	Any cellphone	Smartphone	Cellphone, but not smartphone
Black	94%	72%	23%
Hispanic	98%	75%	23%
Ages 18-29	100%	92%	8%
30-49	99%	88%	11%
50-64	97%	74%	23%
65+	80%	42%	38%
Less than high school graduate	92%	54%	39%
High school graduate	92%	69%	23%
Some college	96%	80%	16%
College graduate	97%	89%	8%
Less than \$30,000	92%	64%	29%
\$30,000-\$49,999	95%	74%	21%
\$50,000-\$74,999	96%	83%	13%
\$75,000+	99%	93%	6%
Urban	95%	77%	17%
Suburban	96%	79%	16%
Rural	94%	67%	27%

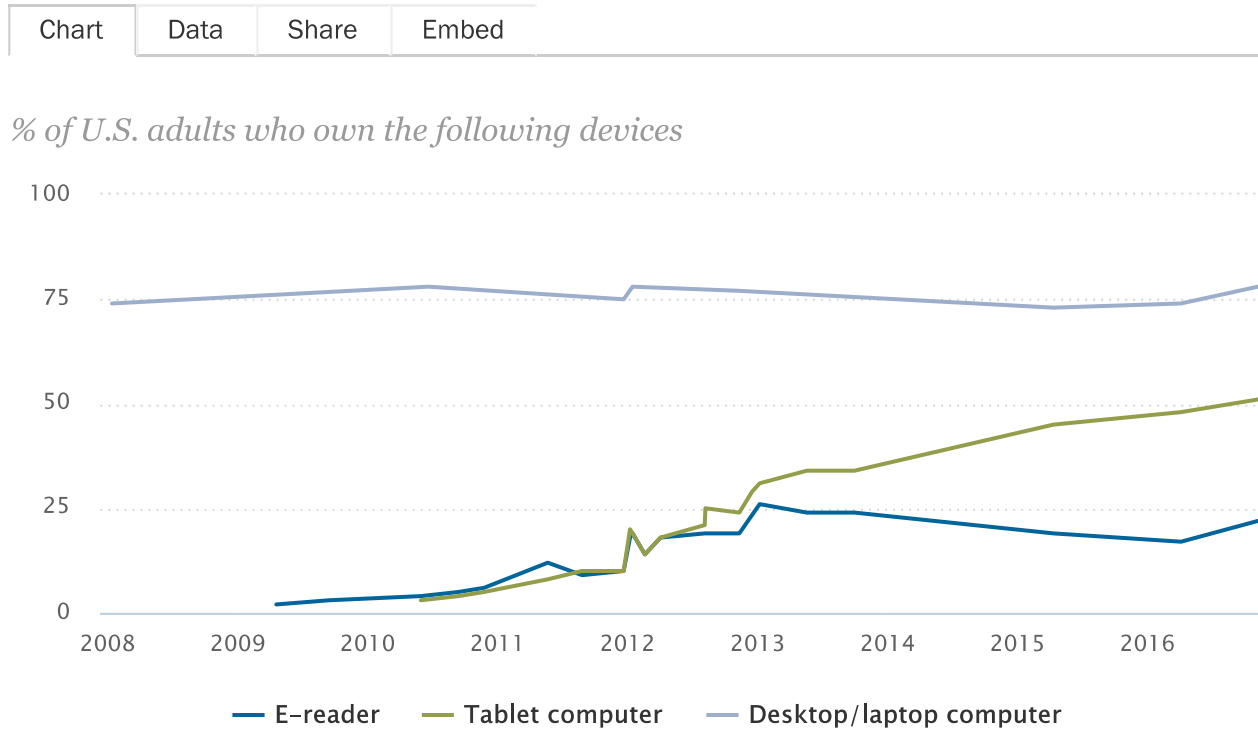
Source: Survey conducted Sept. 29-Nov. 6, 2016.

PEW RESEARCH CENTER



## Ownership of other devices

Along with mobile phones, Americans own a range of other information devices. Nearly eight-in-ten U.S. adults now own desktop or laptop computers, while roughly half now own tablet computers and around one-in-five own e-reader devices.



Source: Surveys conducted 2008-2016.

PEW RESEARCH CENTER

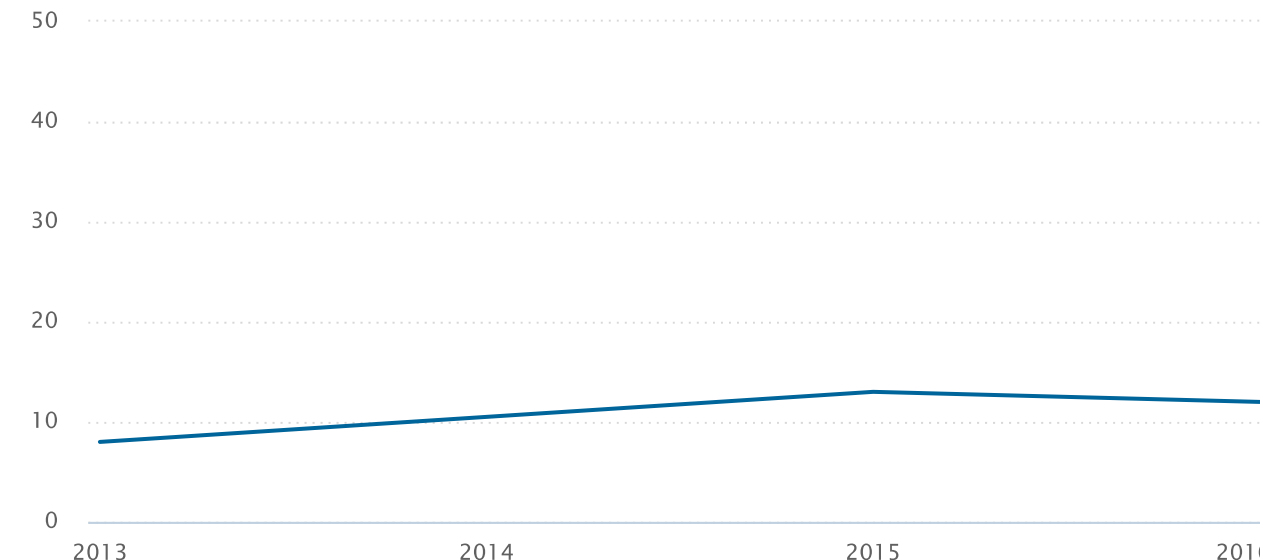


## Smartphone dependency over time

As the adoption of traditional broadband service has slowed in recent years, a growing share of Americans now use smartphones as their primary means of online access at home. Today just over one-in-ten American adults are “smartphone-only” internet users – meaning they own a smartphone, but do not have traditional home broadband service.



## Demographics of Mobile Device Ownership and Adoption in the United States



Source: Surveys conducted 2013-2016. Data for each year based on a pooled analysis of all surveys containing broadband and smartphone questions fielded during that year.

PEW RESEARCH CENTER



## Who is smartphone dependent

Reliance on smartphones for online access is especially common among younger adults, non-whites and lower-income Americans.

Age

Race

Gender

Income

Education

Community

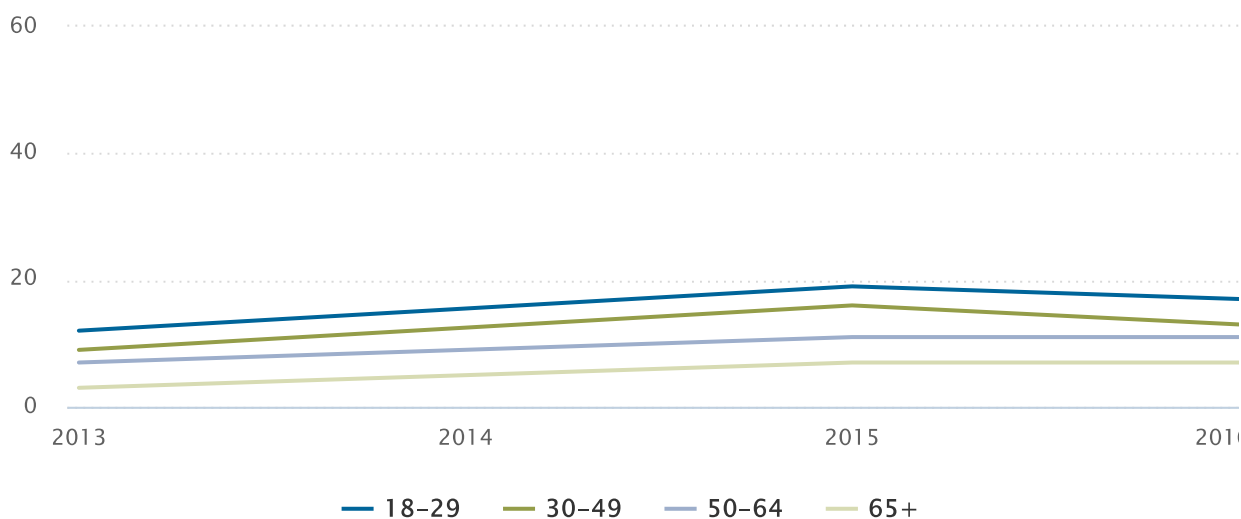
Chart

Data

Share

Embed

## *% of U.S. adults who do not use broadband at home but own smartphones, by age*



Source: Surveys conducted 2013-2016. Data for each year based on a pooled analysis of all surveys containing broadband and smartphone questions fielded during that year.

PEW RESEARCH CENTER



## Find out more

Find more in-depth explorations of the impact of mobile adoption by following the links below.

[Home Broadband 2015: Barriers to broadband adoption](#) Dec. 21, 2015

[Technology Device Ownership 2015](#) Oct. 29, 2015

[U.S. Smartphone Use in 2015](#) April 1, 2015

[All reports and blog posts related to mobile technology](#)

# EXHIBIT D



# Digital Democracy Survey

A multi-generational view of  
consumer technology, media and  
telecom trends

**Ninth edition**

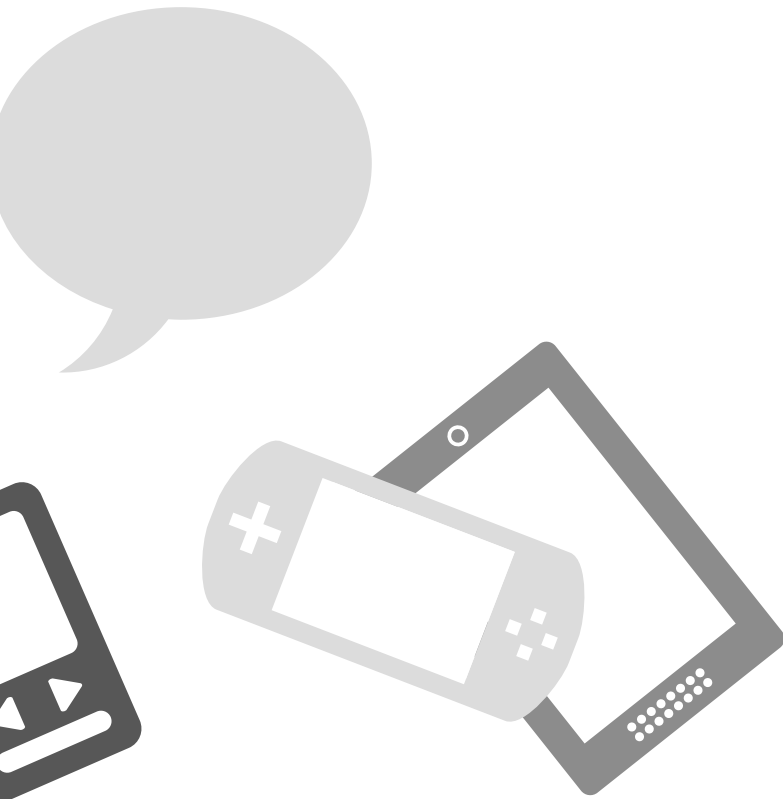
[www.deloitte.com/us/tmttrends](http://www.deloitte.com/us/tmttrends)

#TMTtrends



# Table of contents

4	Preface
5	Product and device landscape
9	The personal viewing experience
9	The <u>mainstreaming</u> of digital
11	Binge-watching
12	Multitasking
14	Viewing preferences
17	The current state of advertising
19	Content originators
20	Personalization of gaming
21	Social media as news
22	About Deloitte's Digital Democracy Survey
23	Contact information



# Preface

The rapidly growing amount of content available via the Internet and the proliferation of devices offering high quality viewing experiences has drastically shifted the way consumers view, access and purchase content.

The ninth edition of Deloitte's Digital Democracy Survey, fielded in November 2014, illustrates consumers' mounting appetite for content — especially video — anywhere, anytime and on any device.

In this executive summary of survey findings, we explore how the adoption of new technologies and devices is changing media consumption habits and preferences among U.S. consumers. These shifts in behavior are particularly insightful when looking at trends by generation.

The notion of consumers sitting in their living rooms to watch television shows at programmed times, especially among younger generations, is quickly giving way to a market of viewers using multiple devices inside and outside the home to consume content when and where they choose to watch. In 2014, there was a shift away from appointment TV to a large number of consumers binge-watching on their own schedules.

With so many new devices and technologies vying for our attention, consumers continue to be distracted while watching TV. The majority of consumers across all generations regularly multitask.

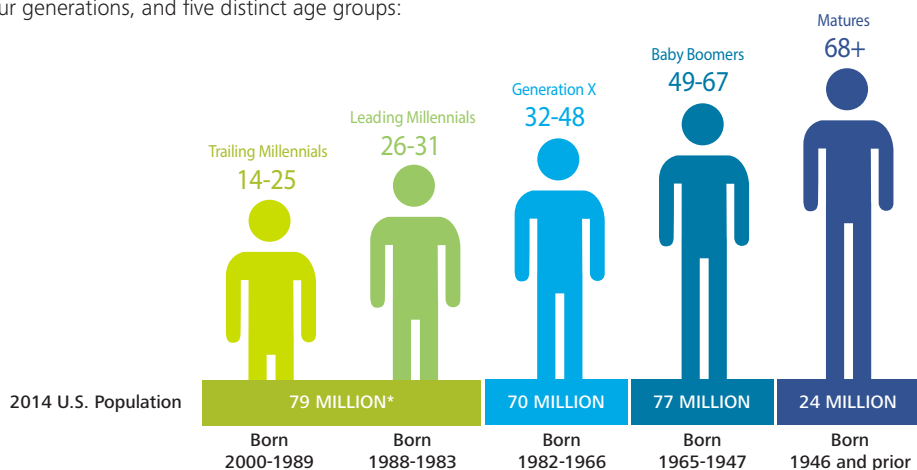
As so much content is being watched outside programmed times and on multiple devices, we'll explore shifts in the effectiveness of traditional and online advertising and the impact of social media on consumer behaviors.

This summary also explores how frequently consumers are using multiple devices to play games and takes a look at how consumers are using gaming consoles for more than just gaming.

Don't see what you're looking for in our executive summary? We've got a lot more data. For more information on Deloitte's Digital Democracy Survey, Ninth Edition, please email us at [tmtrends@deloitte.com](mailto:tmtrends@deloitte.com) and follow us on Twitter @DeloitteTMT.

## TALKING ABOUT THE GENERATIONS

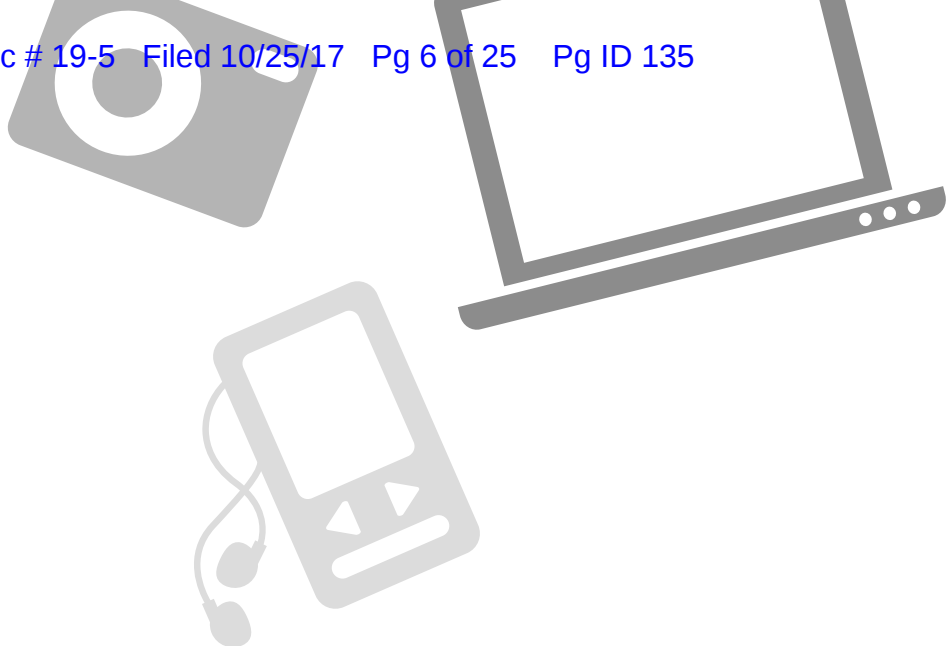
The survey focuses on four generations, and five distinct age groups:



*\*Millennials age 10-13 not included in this study*







Source: 2010 U.S. Census Bureau—Population Division, U.S. Interim Projections 2000-2050

# Product and device landscape



## PRODUCT OWNERSHIP BY U.S. HOUSEHOLD







Flat panel television and smartphone penetration continue to grow among U.S. consumers. Product and device ownership tends to be driven by generational trends, with Trailing Millennials often leading adoption of newer and more mobile technologies.

	 Total 2014		 14-25	 26-31	 32-48	 49-67	 68+
Among Total U.S. Consumers (%)	2013	2014	Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures
Laptop computer	81	82	91	87	88	77	60
Flat panel television	76	82	71	83	86	83	87
Smartphone	65	71	86	84	82	57	40
Desktop computer	71	66	62	58	62	70	83
Gaming console	58	56	80	72	63	40	19
Tablet	48	54	58	48	65	50	37
Digital video recorder (DVR)	51	50	43	45	56	50	54
Streaming media box or over-the-top box	17	18	17	23	25	12	10
Portable streaming thumb drive/fob	7	9	10	10	12	8	2
Fitness band	--	9	9	11	10	9	1
Smart watch	--	3	4	6	3	1	1

**Question:** Which of the following media or home entertainment equipment does your household own?

### TOP THREE MOST VALUED PRODUCTS AMONG OWNERS

Device value is mostly stable year-over-year with the exception of tablets, which appears to be dropping in relative value. Owners place relatively high value on new products, such as smart watches and fitness bands.







	 Total 2014		 14-25  26-31  32-48  49-67  68+				
Top 3 Ranking Among Owners (%)	2013	2014	Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures
Smartphone	72	76	76	78	79	75	65
Laptop computer	67	71	75	68	68	74	59
Flat panel television	62	62	40	53	62	70	80
Desktop computer	55	55	35	46	48	64	86
Basic mobile phone	39	36	13	22	20	50	52
Tablet	36	31	30	35	32	33	22
Gaming console	31	27	45	30	20	13	7
Digital video recorder (DVR)	20	22	11	15	25	24	29
Smart watch	--	18	^	^	^	^	^
Streaming media box or OTT box	18	15	13	24	18	10	2
Fitness band	--	14	^	^	^	^	^
Portable video game player	9	10	16	20	1	6	0
Portable streaming thumb drive/fob	5	6	^	^	^	^	^

^ base too small to show

**Question:** Of the products you indicated you own, which 3 do you value the most?

### INTENT TO PURCHASE IN THE NEXT 12 MONTHS AMONG NON-OWNERS

Although non-owners place TVs, laptops and tablets among the most highly ranked products to purchase in the next year, new technologies are showing substantial promise, especially with Millennials and Xers.

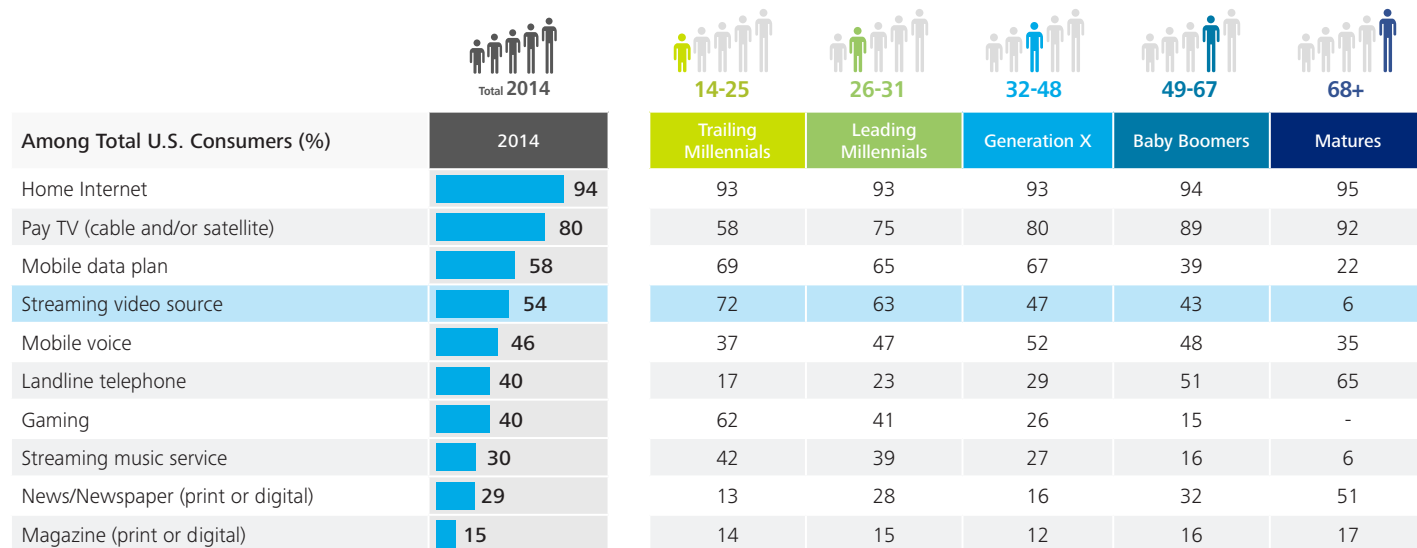
	 Total 2014		 14-25  26-31  32-48  49-67  68+				
Among Total U.S. Consumers (%)	2014		Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures
Flat panel television	30		22	25	35	39	19
Laptop computer	22		50	25	23	20	11
Tablet	22		27	23	28	17	15
Smartphone	19		28	23	24	18	10
Fitness band	11		12	14	15	8	3
Smart watch	10		13	17	13	6	1
Streaming media box or over-the-top box	9		11	12	15	6	2
Portable streaming thumb drive/fob	7		7	10	12	4	1
3D printer	6		7	8	7	6	1

**Question:** Of the products you indicated you do not currently own, which of the following do you plan to purchase in the next 12 months?

## Product and device landscape

## TOP THREE MOST VALUED SERVICES AMONG SUBSCRIBERS

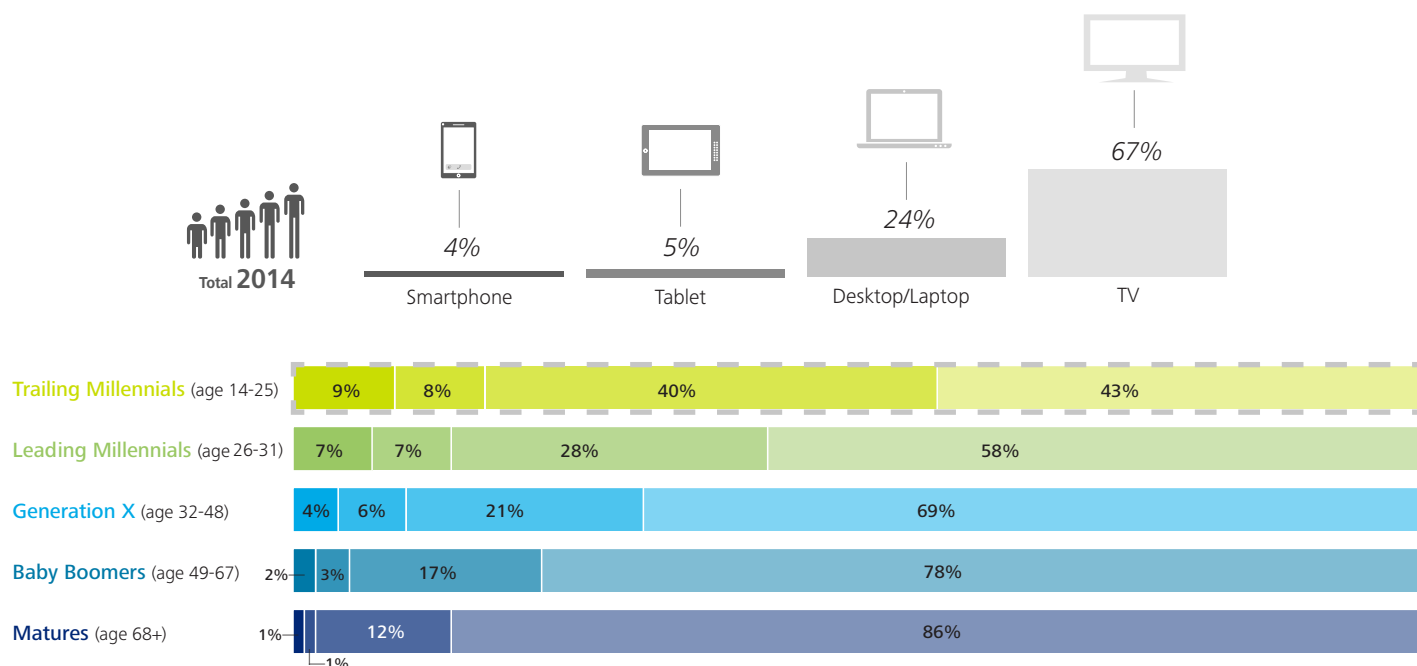
Home Internet is overwhelmingly the most valued service across all generations, with nearly all consumers ranking it in their top three. Pay TV's value is decidedly age-dependent. Trailing Millennials do not value it nearly as much as the other generations. Conversely, streaming services are highly valued among Millennials.



**Question:** Of the services you indicated your household purchases, which three do you value the most?

## PERCENTAGE OF TIME SPENT WATCHING MOVIES BY DEVICE AMONG U.S. CONSUMERS

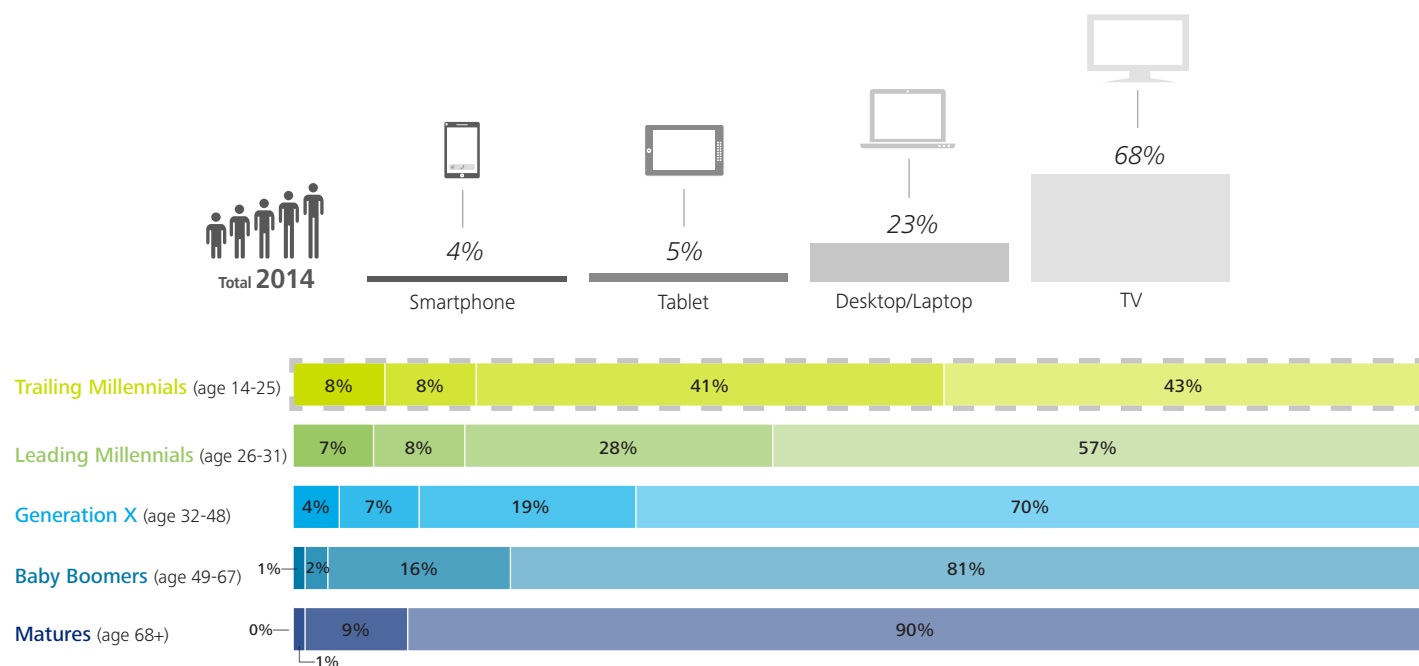
Although TV ownership remains strong and is growing, content is increasingly being viewed on platforms other than televisions. Movie viewing habits are categorically age-dependent. Among Trailing Millennials, nearly 60% of time spent watching movies occurs on computers, tablets, or smartphones.



**Question:** Of the time you spend watching movies, what percentage of time do you watch on the following devices?

## PERCENTAGE OF TIME SPENT WATCHING TV SHOWS BY DEVICE AMONG U.S. CONSUMERS

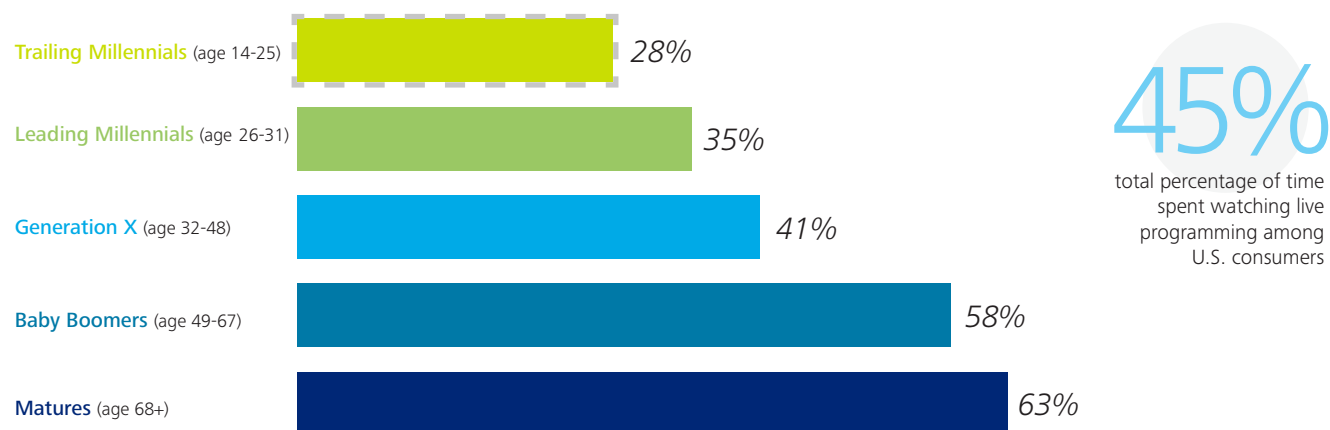
The same pattern applies to watching TV shows. Older viewers rely on televisions, while younger viewers have moved to computers and mobile devices. Trailing Millennials spend more time watching TV shows on non-traditional devices than on televisions.



**Question:** Of the time you spend watching TV shows (e.g., 30- or 60-minute television programs), what percentage of time do you watch on the following devices?

## PERCENTAGE OF TIME SPENT WATCHING LIVE PROGRAMMING AMONG U.S. CONSUMERS

When taking into account that Trailing Millennials spend more time watching TV shows on non-traditional devices than on televisions, it's not surprising that only a quarter of television programming they watch is done live at the time of broadcast. The percentage of programming watched live increases by age.



**Question:** When watching television content, what percent of time are you watching the following methods of programming?














# The personal viewing experience



## The mainstreaming of digital

### FREQUENCY OF STREAMING, RENTING AND PURCHASING MOVIES

Heavily driven by the adoption of streaming services among younger generations, the majority of consumers stream movies at least monthly. More than half of all consumers and three-quarters of Millennials stream movies on a monthly basis. When compared to weekly frequency, streaming dominates, with 34% of all consumers and 57% of Trailing Millennials streaming movies weekly. Though streaming is the norm, physical discs are not irrelevant. Almost half of consumers rent or buy physical discs on a monthly basis.

		 Total 2014	 Total 2014	 14-25	 26-31	 32-48	 49-67	 68+
Among Total U.S. Consumers (%)	Weekly	At least monthly	Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures	
 Online Streaming Service	34	56	77	71	65	40	23	
 Rent DVD/Blu-Ray	10	35	40	47	40	29	17	
 Purchase DVD/Blu-Ray	6	29	36	40	30	25	14	
 Purchase/Rent via On Demand/ Pay-Per-View	6	26	28	34	31	22	12	
 Purchase Digital Download	5	23	31	36	28	13	6	
 Rent Digital Download	5	21	31	32	25	14	4	

**Question:** Thinking about how you watch movies, how frequently do you do each of the following?












**34%** of U.S. consumers stream movies on a *weekly* basis

**57%** of Trailing Millennials stream movies on a *weekly* basis

**48%** of U.S. consumers rent or buy *physical* discs monthly

## FREQUENCY OF STREAMING, RENTING AND PURCHASING TV SHOWS

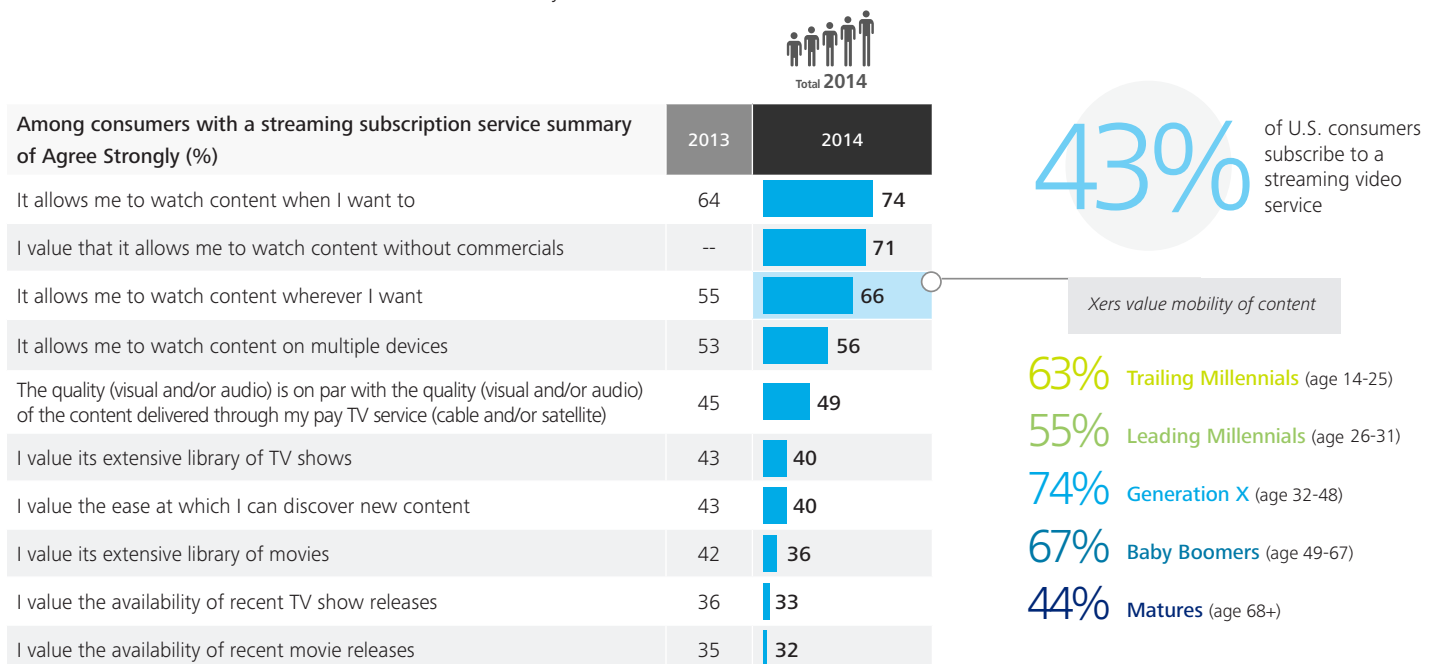
Consumption patterns are similar for television programming; Trailing Millennials overwhelmingly stream, with approximately three-quarters using a streaming service on a monthly basis to watch television programs. Although older consumers have not adopted streaming at quite the same pace, it is still the most frequent method of renting/purchasing television content among those groups.

		 Total 2014	 14-25	 26-31	 32-48	 49-67	 68+
Among Total U.S. Consumers (%)	At least monthly		Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures
 Online Streaming Service	53		72	69	60	38	23
 Rent DVD/Blu-Ray	28		31	36	31	24	14
 Purchase/Rent via On Demand/ Pay-Per-View	24		22	35	29	20	10
 Purchase DVD/Blu-Ray	23		29	33	26	19	9
 Purchase Digital Download	19		26	31	23	11	5

**Question:** Thinking about how you watch television programming, how frequently do you do each of the following?

## CONSUMER PERCEPTIONS OF THEIR STREAMING SERVICES

The reasons behind why people stream are clear. Consumers appreciate their streaming services for the ease with which they can watch commercial-free content anytime, anywhere, and on any device. Xers have a particular interest in the mobility of their content, with three-quarters saying they stream because it allows them to watch content where they want.











**Question:** Please indicate how much you agree or disagree with the following statements about your streaming video service.

The personal viewing experience

# Binge-watching







## PERCENTAGE OF U.S. CONSUMERS WHO BINGE-WATCH TV SHOWS

Two-thirds of viewers “binge-watch” TV, watching three or more episodes of TV in one sitting. Millennials overwhelmingly engage in binge-watching behaviors. Not surprisingly, binge-watching is much more common among those who have a streaming subscription, but even those who don’t have a streaming service still binge, likely via a DVR. Trailing Millennials binge-watch more frequently than any other generation, with 42% binge-watching on a weekly basis.

	 Total 2014	 14-25	 26-31	 32-48	 49-67	 68+		
Among Total U.S. Consumers (%)	2014	Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures	Have Streaming Subscription	No Streaming Subscription
Ever Binge	68	84	83	74	56	37	83	57

**Question:** Do you ever “binge-watch” television shows, meaning watching three or more episodes of a TV series in one sitting?









## FREQUENCY OF BINGE-WATCHING

	 Total 2014	 14-25	 26-31	 32-48	 49-67	 68+
Among Binge-Watchers (%)	Total 2014	Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures
At least once a week	31	42	30	25	29	26
At least once a month	34	35	40	38	28	24
At least every six months	27	19	23	27	35	29
At least once a year	8	4	8	11	8	21

**Question:** How frequently do you “binge-watch” television shows?

## MOST BINGED GENRE

TV drama is the most popular television genre to binge-watch, as a continuous narrative lends itself well to multi-episode viewing. Comedies are the second most popular genre to binge-watch, with a sharp drop after that. There are some gender differences among binge-watchers, with women being more likely to binge on dramas and men being more likely than women to binge on comedies.

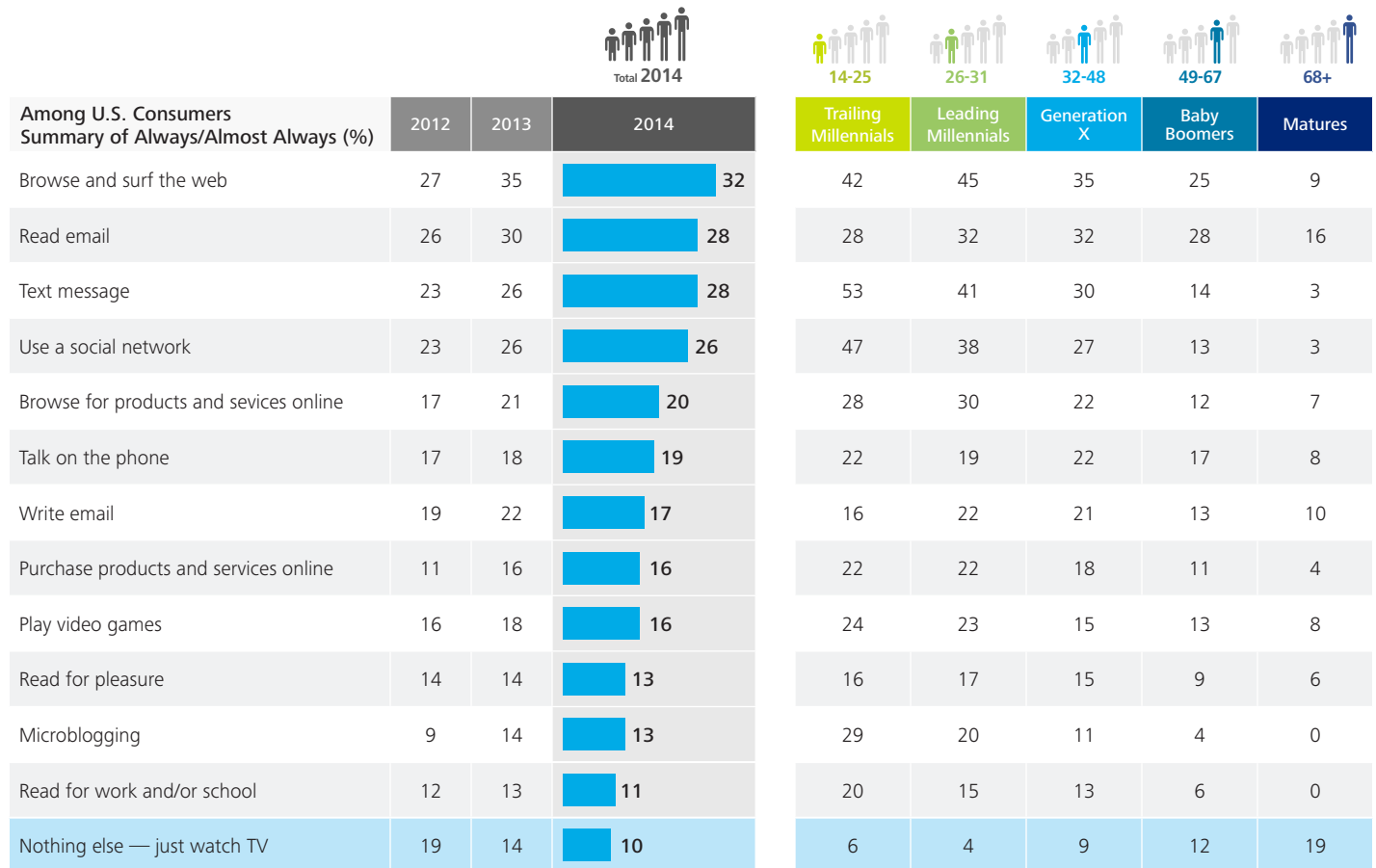
	 Total 2014	 14-25	 26-31	 32-48	 49-67	 68+	 Male	 Female
Among Total U.S. Consumers (%)	2014	Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures	Male	Female
TV drama	54	49	54	58	57	53	51	58
TV comedy	20	25	23	19	16	11	24	16
Reality TV show	7	8	7	8	6	4	5	9
Contest show	3	2	2	2	4	2	3	2
Daytime shows	2	2	3	2	3	5	2	3
Variety/talk shows	1	1	1	1	0	1	1	1
Do It Yourself (DIY)/Cooking shows	4	2	3	6	6	3	4	4
None of the above	9	11	8	5	8	21	10	7

**Question:** When you “binge-watch,” what kind of show are you most often watching?

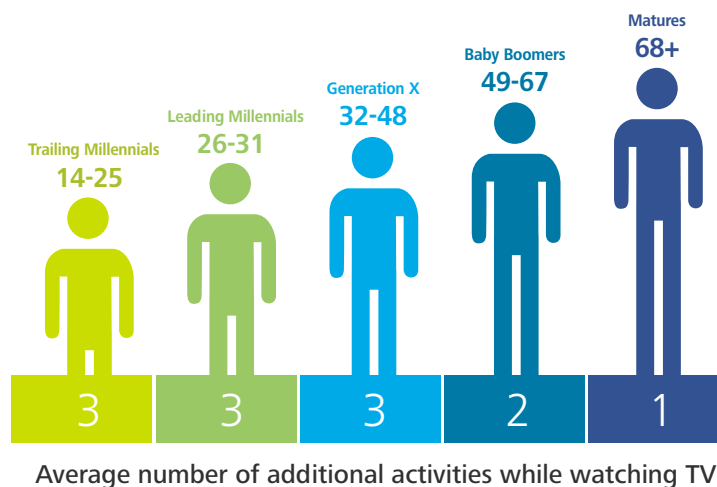
# Multitasking

## PERCENTAGE OF U.S. CONSUMERS WHO MULTITASK WHILE WATCHING TV

Ninety percent of consumers are multitasking while watching TV. On average, Millennials and Xers are doing three additional activities while watching TV, typically surfing the web, emailing, texting, or social networking.



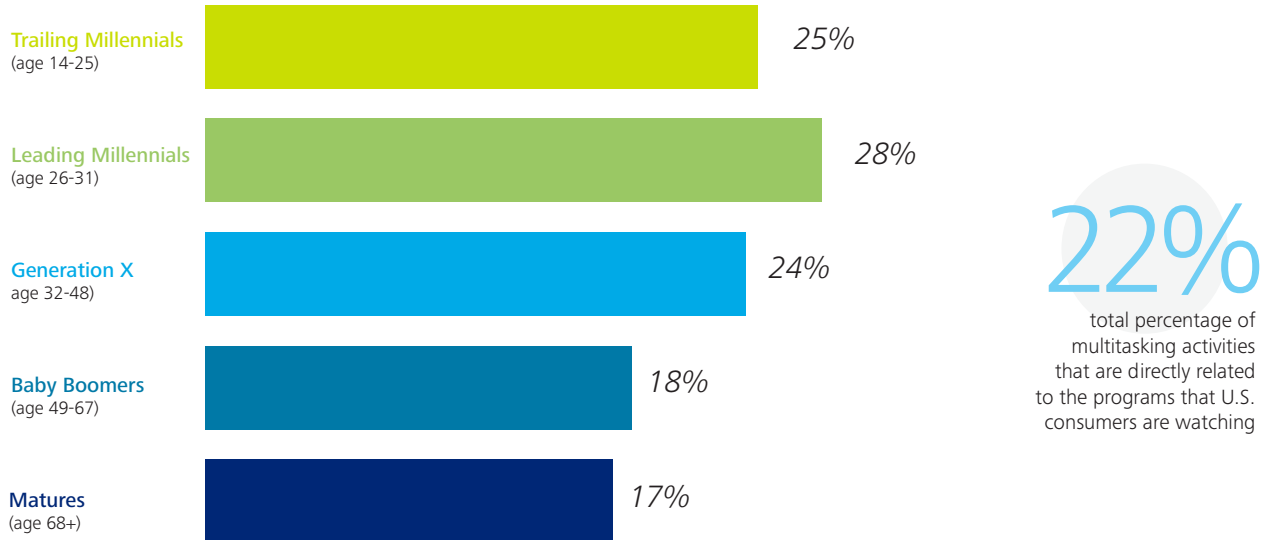
**Question:** Which are things you typically do while watching your home TV?



The personal viewing experience

### PERCENTAGE OF MULTITASKING DIRECTLY RELATED TO THE PROGRAM

Despite the high percentage of consumers who are multitasking while watching TV, fewer than one-quarter of multitasking activities are directly related to the programs that consumers are watching.

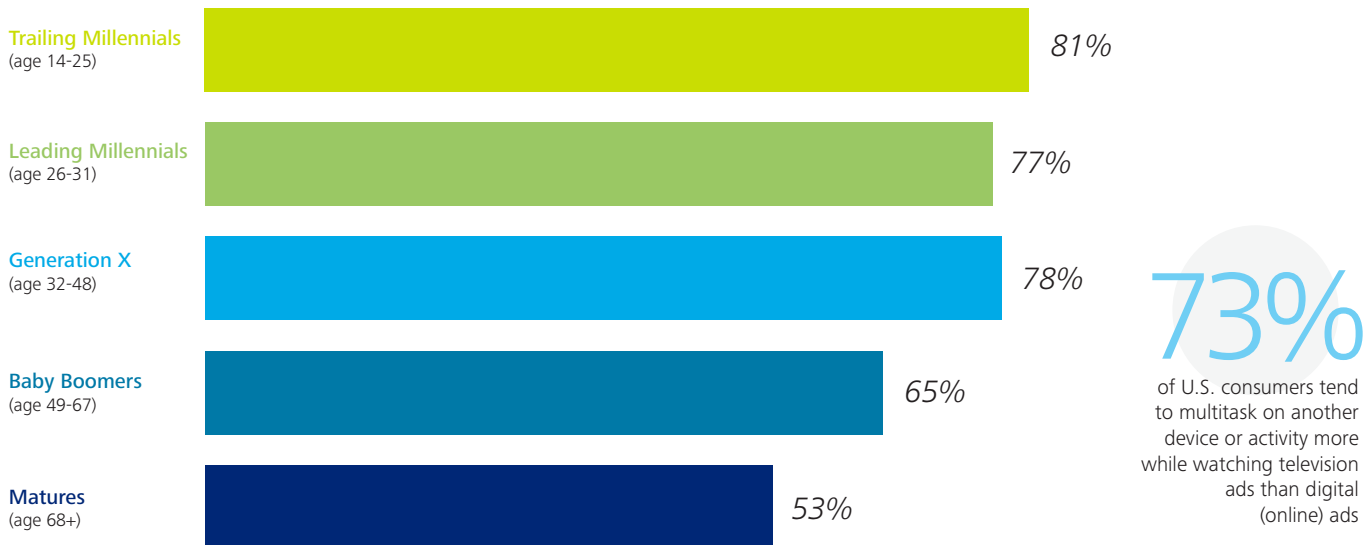


**Question:** What percentage of your multitasking activities are directly related to the program you are watching?

### INTENSITY OF ATTENTION RELATED TO DIGITAL ADS

When compared to traditional TV advertising, consumers tend to pay more attention to digital (online) ads. Four out of five Millennials are more distracted during TV ads than digital.

*I tend to multitask on another device or activity more while watching television ads than digital (online) ads:*

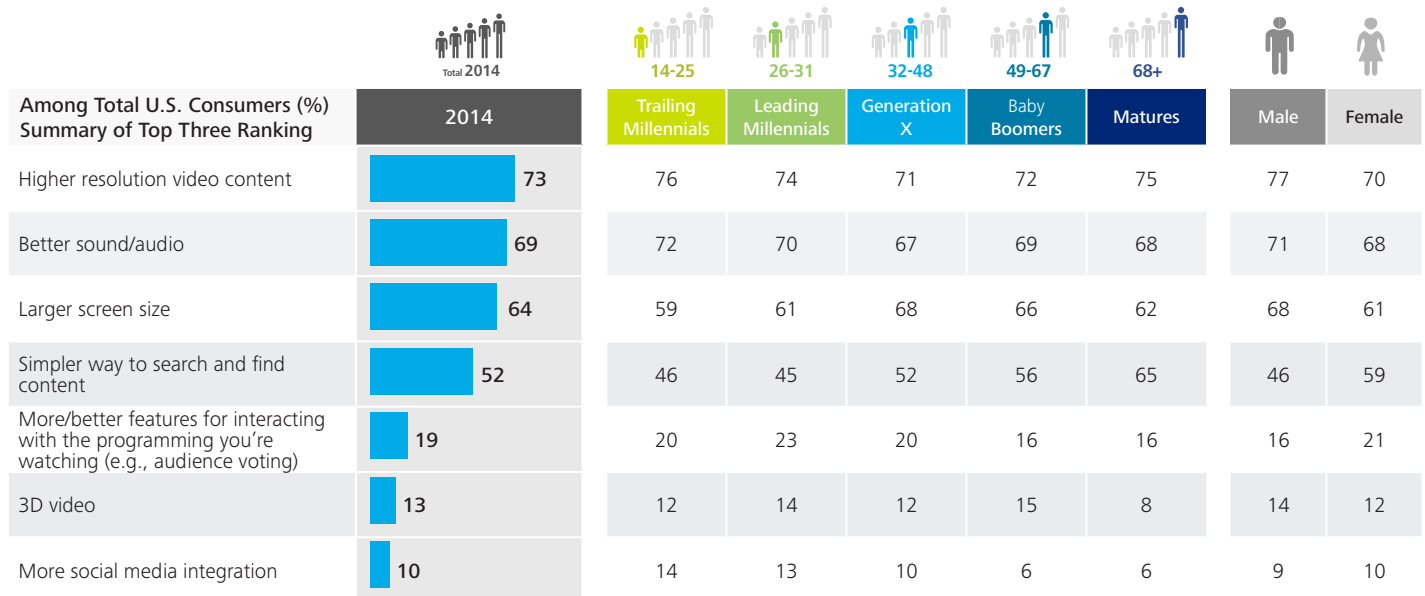


**Question:** Thinking about advertisements that come on during television or digital (online) programming you watch, please rate the following statements using the scale below.

# Viewing preferences

## TOP THREE FEATURES IMPROVING VIEWING EXPERIENCE

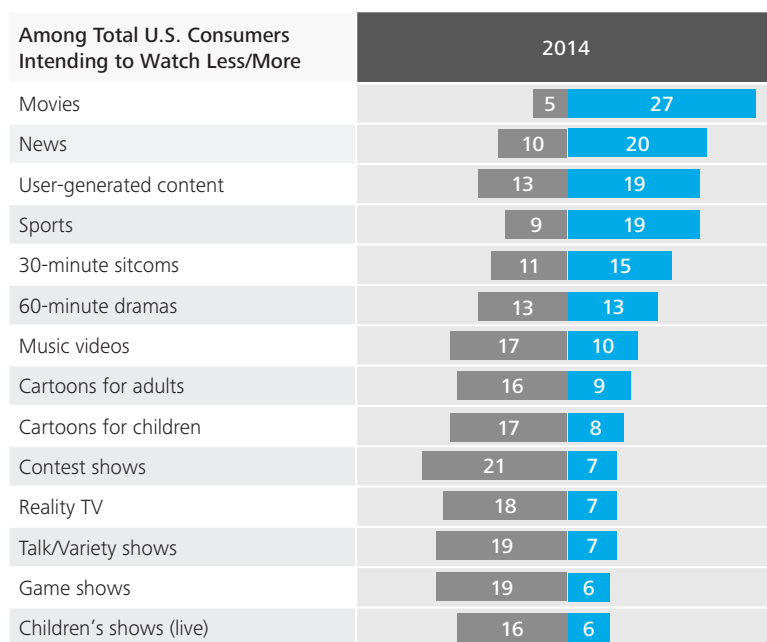
Video and audio quality are universally the most important factors in improving viewing experience, with screen size also playing a significant role. However, there are significant gender preferences, with males appreciating higher resolution and screen size more, and females showing an interest in a simpler way to search and find content.



**Question:** Thinking about the entertainment content you watch at home, which three characteristics would improve your viewing experience the most?

## VIDEO CONSUMPTION BY GENRE

Movies will continue to outpace all other video genres in the next 12 months. Consumers are generally less selective in choosing movies than TV programming due to the time commitment of a full television series season. Trailing Millennials may choose their TV series even more carefully than older generations.



**Question:** Thinking about your consumption of video content and programming, do you think you will watch more, about the same, or less of each of the following types of video content in the next 12 months?

## PREFERENCES RELATED TO MOVIE AND TV VIEWING

68%

of U.S. consumers are more selective in watching television series than movies because television series are a full season commitment

76% Trailing Millennials (age 14-25)

72% Leading Millennials (age 26-31)

67% Generation X (age 32-48)

61% Baby Boomers (age 49-67)

65% Matures (age 68+)

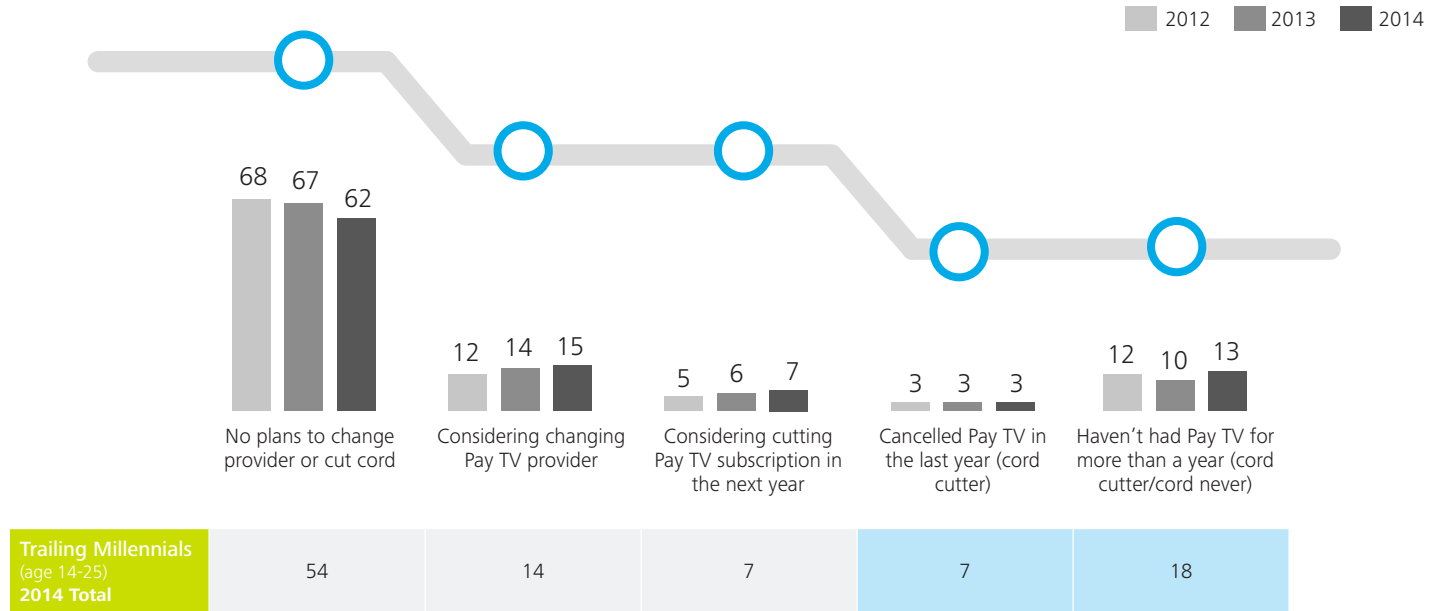
Less  
More

**Question:** Please indicate how much you agree or disagree with the following statements.

The personal viewing experience

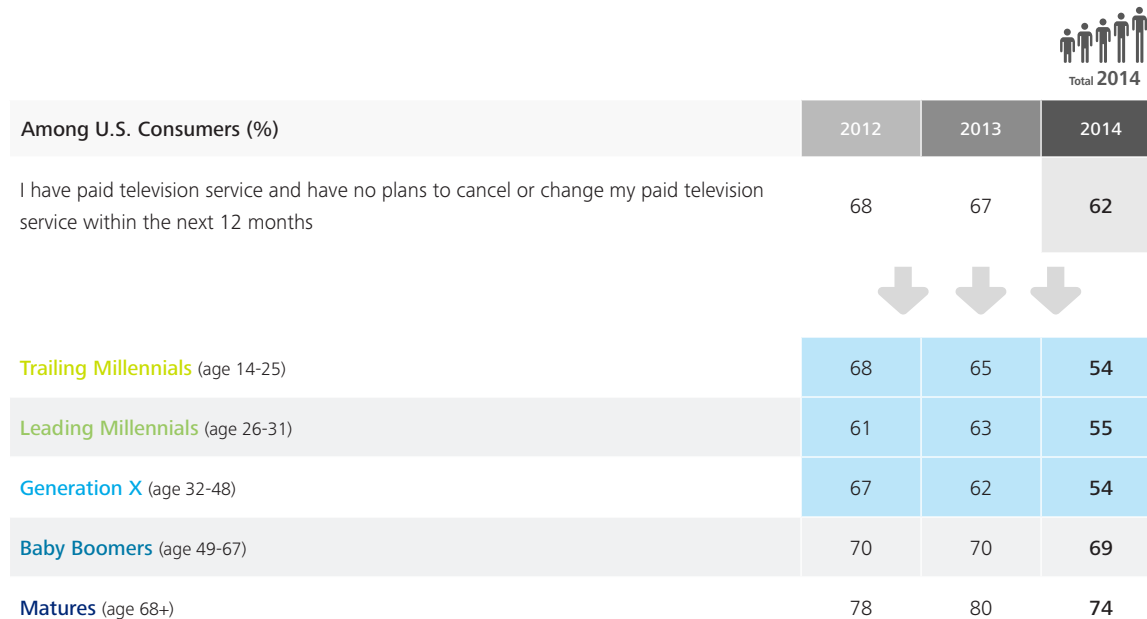
## PAY TV SUBSCRIPTION ROADMAP

There was a decrease in the number of Pay TV subscribers that say they have no plans to change providers or cut the cord this year. A quarter of Trailing Millennials either cancelled their Pay TV subscriptions in the last 12 months or haven't had Pay TV for more than a year. This trend is more pronounced among the older Trailing Millennials aged 19-25 than the younger 14-18 year olds.



## INTEREST IN CHANGING OR CANCELLING PAY TV SERVICE

Millennials and Xers are significantly more open to change, with only about half saying they have no plans to change.



## PAY TV SUBSCRIPTION PREFERENCES

Consumers are increasingly interested in purchasing TV channels in à la carte packages, with over half saying they prefer to subscribe only to the channels they watch regularly. The trend is consistent across the generations, and occurs in parallel with a decrease in the number of channels watched on average.

	Total 2014			14-25	26-31	32-48	49-67	68+
Among Total U.S. Consumers with Pay TV Service (%)	2012	2013	2014	Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures
Subscribe only to the channels I watch regularly	42	47	52	52	49	54	51	53
Subscribe to a package of channels even if I do not regularly watch them all	50	47	40	39	42	43	40	38
Purchase only those individual shows and events I want to watch	8	6	8	9	9	4	9	9

**Question:** In terms of how you purchase paid television, what would be your preference of the choices listed below?

## AVERAGE NUMBER OF CHANNELS WATCHED

	Total 2014			14-25	26-31	32-48	49-67	68+
Among Total U.S. Consumers with Pay TV Service (%)	2012	2013	2014	Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures
Average Number of Channels	15	13	11	9	11	11	12	10

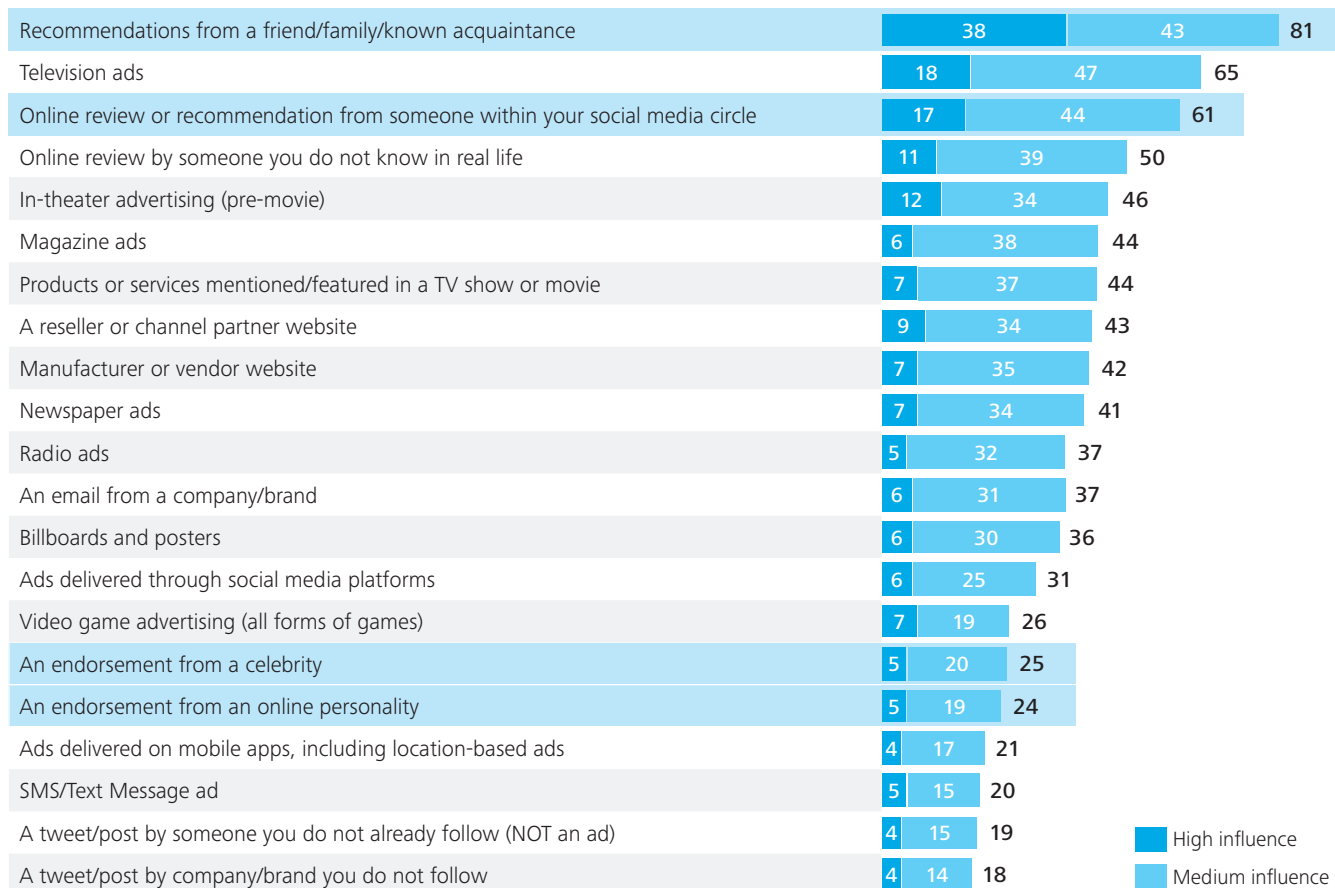
**Question:** Think about the channels you watch on your paid television service. How many channels do you watch regularly?

# The current state of advertising



## BUYING DECISION INFLUENCE

Personal recommendations, including those from within social media circles, play a major role in buying decisions. Interestingly, consumers say that an endorsement from an online personality is just as influential as one from a celebrity.

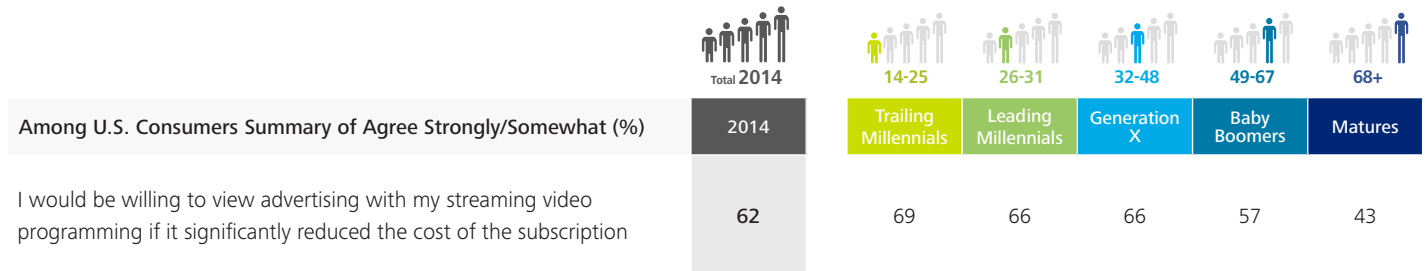


**Question:** To what degree do the following influence your buying decisions?

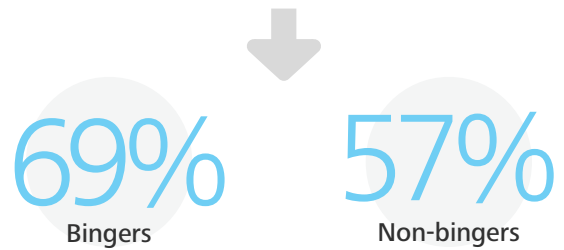
## ADVERTISING AND STREAMING SERVICES

Consumers show a willingness to endure advertising in exchange for discounted content. Two-thirds of consumers say they would be willing to view advertising with streaming video programming if it significantly reduced the cost of the subscription.

Bingers have a higher willingness to endure advertising in exchange for discounted content with 69% of bingers saying they would be willing to view advertising with their streaming video advertising if it significantly reduced the cost of their subscription.

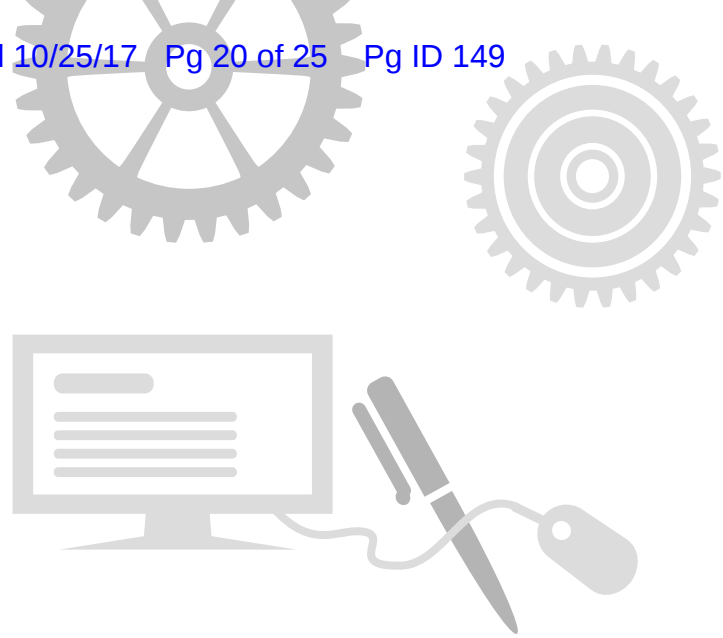


*Question: Please indicate how much you agree or disagree with the following statements.*



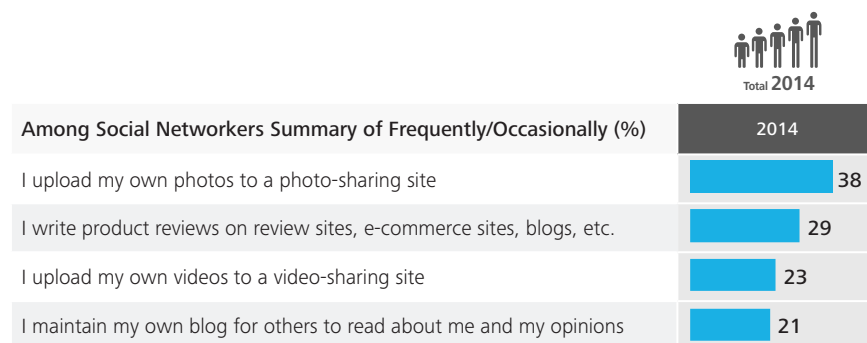
*Willingness to view advertising with streaming video if it significantly reduced cost of subscription*

# Content originators



## BUYING DECISION INFLUENCE







Eight percent of consumers are “Content Originators,” meaning they actively upload photos and videos, write reviews, and maintain blogs. Content Originators are bigger consumers of content in all forms, but especially movies – close to 90% stream movies on a monthly basis as compared to just half of non-Content Originators. They also purchase/rent far more on-demand and digital downloads.



**8%**  
of U.S. consumers are “core” Content Originators, meaning they do all of the four activities

**Question:** Thinking about social networking, how frequently do you do each of the following?

## FREQUENCY OF STREAMING, RENTING AND PURCHASING MOVIES

Summary of Frequently/Occasionally (at least monthly) (%)		2014	Content Originator	Non-Content Originator
	Online Streaming Service	56	88	53
	Purchase/Rent via On Demand/Pay-Per-View	26	77	21
	Rent Digital Download	21	72	17
	Purchase Digital Download	23	71	18
	Rent DVD/Blu-Ray	35	69	32
	Purchase DVD/Blu-Ray	29	69	26

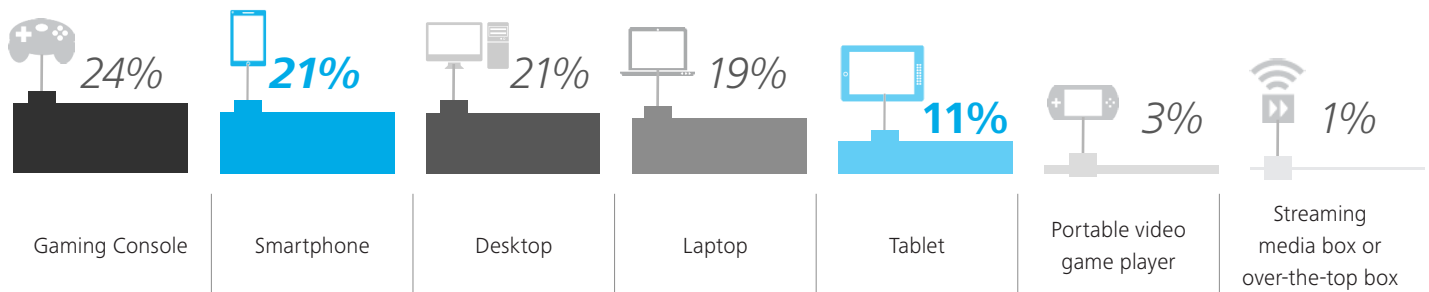
**Question:** Thinking about how you watch movies, how frequently do you do each of the following?

# Personalization of gaming



## SHARE OF TIME SPENT ON GAMING PLATFORMS

Almost 40% of U.S. Consumers and 54% of Trailing Millennials play video games on a daily or weekly basis. Gamers are spending a third of their playing time on mobile platforms (smartphones and tablets), perhaps because of the proliferation of casual games (e.g. puzzles and word games). Gaming consoles are increasingly being used for content consumption, especially watching/ streaming movies.



**Question:** Of the time you spend playing games (all types of games), what percentage of time do you play games on the following devices?

## CONSOLE USAGE



## GAMING FREQUENCY

Among Those With Consoles (%) activities performed on gaming console	2013	2014
<b>Summary of Top 3 Ranking</b>		
Play video games	88	86
Watch movies (Blu-ray/DVD)	42	48
Stream TV/Movie content	32	38
Watch online content	26	29
Browse the Internet	16	16
Fitness training/education	16	15
Stream music	12	15
View home videos/photos	7	7

**Question:** What top three activities are you doing on your gaming console?

38%

of U.S. consumers play games at least weekly

54%

of Trailing Millennials play games at least weekly

**Question:** How often do you play videogames (regardless of type, include mobile, console, phone-based, laptop and/or desktop, and tablet-based games)?







# Social media as news




## MOST POPULAR NEWS PLATFORMS

While television is still the top mechanism for getting news, its importance has been decreasing over the last several years. Social media sites are becoming a primary source of news for Trailing Millennials.

	 Total 2014			 14-25	 26-31	 32-48	 49-67	 68+
Among Total U.S. Consumers (%)	2012	2013	2014	Trailing Millennials	Leading Millennials	Generation X	Baby Boomers	Matures
Television	57	49	48	28	40	45	61	70
Online news sites not associated with a newspaper	17	19	12	15	10	13	11	4
Social media sites	4	9	11	26	15	10	3	1
Online version of newspapers	9	10	10	7	16	13	8	4
Print newspapers	6	6	7	3	4	5	10	15
Radio	3	4	5	5	3	7	5	2
Variety/talk shows	—	—	2	4	5	1	0	0
News aggregators	—	—	2	3	3	3	1	0
I do not follow the news	3	4	4	8	5	3	2	3

*Question: Which of the following is your most frequently used mechanism to get news?*

# About Deloitte's Digital Democracy Survey

- This is the ninth edition of research commissioned by Deloitte's Technology, Media and Telecommunications (TMT) practice.
- Focusing on four generations and five distinct age groups, the survey provides insight into how consumers ages 14 and above are interacting with media, products and services, mobile technologies, the Internet, attitudes and behaviors toward advertising and social networks—and what their preferences might be in the future.
- Fielded by an independent research firm from 11/3/2014 to 11/19/2014, the survey employed an online methodology among 2,076 U.S. consumers.
- All data is weighted back to the most recent census data to give a representative view of what U.S. consumers are doing.
- For meaningful changes, we look for differences in year-over-year tracking and generations of at least five percentage points.

# Contact information



**Gerald Belson**

Principal and U.S. Media &  
Entertainment Sector Leader  
Deloitte Consulting LLP  
gbelson@deloitte.com



**Paul Sallomi**

Partner and U.S. Technology  
Sector Leader  
Deloitte Tax LLP  
psallomi@deloitte.com



**Kevin Westcott**

Principal and U.S. Media &  
Entertainment Consulting Leader  
Deloitte Consulting LLP  
kewestcott@deloitte.com



**Craig Wigginton**

Partner and U.S.  
Telecommunications Sector Leader  
Deloitte & Touche LLP  
cwigginton@deloitte.com

## FOR MEDIA INQUIRIES

### **Anisha Sharma**

Technology, Media & Telecommunications Public Relations  
+1 201 290 9119  
anishsharma@deloitte.com

Follow the conversation at @DeloitteTMT

As used in this document, "Deloitte" means Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Member of Deloitte Touche Tohmatsu Limited



# EXHIBIT E

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

*Matthew B. Kugler*<sup>†</sup>

*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*<sup>1</sup>

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

Subject 189<sup>2</sup>

### INTRODUCTION

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

---

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

<sup>1</sup> 541 US 149, 153 (2004).

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

<sup>3</sup> US Const Amend IV.

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

agents unfettered discretion to search the contents of electronic devices?

A recent court opinion proposed that such searches should require an elevated level of suspicion; border agents would not be able to conduct the search unless they had some specific reason to suspect the traveler of wrongdoing.<sup>5</sup> Scholars advocating for this type of elevated-suspicion standard base their arguments on the role that electronic devices now play in daily life, the degree of intrusion into the privacy and dignity of the individuals being searched, and the potential for surprise.<sup>6</sup> Courts have recognized the importance of these factors in evaluating the reasonableness of border searches, particularly the degree of intrusion on privacy and dignity interests.<sup>7</sup> When applying these criteria to searches of electronic devices, however, courts have disagreed on the magnitude of the privacy intrusion. In *United States v Cotterman*,<sup>8</sup> 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.”<sup>9</sup> Based on this assessment, the Ninth Circuit then concluded that some searches of electronic devices represent a “substantial intrusion” on privacy and dignity and should therefore require elevated suspicion.<sup>10</sup> Other courts, however, have disputed the notion that travelers find searches of electronic devices any more intrusive or surprising than searches of their other possessions and have therefore not reached the same result.<sup>11</sup>

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

---

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

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

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

<sup>8</sup> 709 F3d 952 (9th Cir 2013).

<sup>9</sup> Id at 967.

<sup>10</sup> Id at 968.

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

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

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

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

---

<sup>12</sup> See notes 51–54 and accompanying text.

<sup>13</sup> See Table 1.

<sup>14</sup> See text accompanying notes 68–85.

<sup>15</sup> See pp 1195–96.

<sup>16</sup> See *Cotterman*, 709 F3d at 967.

<sup>17</sup> No 13-132, slip op (US June 25, 2014).

<sup>18</sup> 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).

<sup>19</sup> *Riley*, No 13-132, slip op at 8–10.

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

## I. THE BORDER SEARCH EXCEPTION

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

“A search or seizure is ordinarily unreasonable” absent “individualized suspicion of wrongdoing;” the police cannot simply enter and search your house.<sup>20</sup> 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.<sup>21</sup> Border searches have historically been viewed as one exception to the individualized-suspicion requirement. Routine border searches can occur absent any individualized suspicion because “[t]he Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.”<sup>22</sup> Nonroutine, more invasive searches may require a showing of a low level of individualized suspicion called “reasonable suspicion.”<sup>23</sup>

### A. History of the Exception

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

---

<sup>20</sup> *City of Indianapolis v Edmond*, 531 US 32, 37 (2000).

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

<sup>22</sup> *United States v Flores-Montano*, 541 US 149, 152 (2004).

<sup>23</sup> *United States v Montoya de Hernandez*, 473 US 531, 541 (1985).

<sup>24</sup> Act of July 31, 1789 § 24, 1 Stat 29, 43, repealed by Act of Aug 4, 1790 § 74, 1 Stat 145, 178.

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

The main wave of modern border search cases has concerned the smuggling of controlled substances. In the Prohibition-era case *Carroll v United States*,<sup>27</sup> the Court used the border search doctrine as a point of comparison in devising a new exception to the warrant requirement for the search of automobiles.<sup>28</sup> The *Carroll* Court said that “[t]ravelers may be so stopped [without cause] in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in.”<sup>29</sup> Automobile searches, in contrast, were held to require probable cause (though not a warrant) because the state does not have the same set of strong interests in the nation’s interior that it does at the border, where a search is presumptively reasonable even without probable cause.<sup>30</sup>

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

---

<sup>25</sup> Act of July 31, 1789 § 24, 1 Stat at 43.

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

<sup>27</sup> 267 US 132 (1925).

<sup>28</sup> See *id.* at 153–54. The case concerned the smuggling of alcohol during Prohibition. See *id.* at 159–60.

<sup>29</sup> *Id.* at 154.

<sup>30</sup> See *id.*

<sup>31</sup> 431 US 606 (1977).

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

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

#### B. Requirement of Reasonable Suspicion for Nonroutine Searches

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

---

<sup>32</sup> Id at 620.

<sup>33</sup> Id at 609.

<sup>34</sup> Id at 611, quoting 19 USC § 482.

<sup>35</sup> *Ramsey*, 431 US at 616.

<sup>36</sup> See id at 623–24.

<sup>37</sup> See id at 623.

<sup>38</sup> See id at 624.

The term “reasonable suspicion” has its origin in the *Terry v Ohio*<sup>39</sup> investigative stop case.<sup>40</sup> It is defined as “a particularized and objective basis for suspecting the particular person stopped of criminal activity.”<sup>41</sup> 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.’”<sup>42</sup> Reasonable suspicion generally cannot be based purely on demographic characteristics, but it can be found if the suspect fits a detailed offender profile.<sup>43</sup>

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

---

<sup>39</sup> 392 US 1, 37 (1968).

<sup>40</sup> *Id.*

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

<sup>42</sup> *Terry*, 392 US at 27.

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

<sup>44</sup> 473 US 531 (1985).

<sup>45</sup> *Id.* at 532.

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

<sup>47</sup> *Id.* at 534.

<sup>48</sup> *Montoya de Hernandez*, 473 US at 534–35.

<sup>49</sup> *Id.* at 535.

<sup>50</sup> *Id.* at 534–36.

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

The general rule from *Montoya de Hernandez* is that the reasonableness of a search is determined by balancing the intrusion on the individual’s Fourth Amendment interests against governmental interests.<sup>55</sup> 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.”<sup>56</sup> At the border, however, the test is “qualitatively different” in that the balancing of interests is struck “much more favorably to the Government.”<sup>57</sup> This is why routine border searches are not subject to any requirement of reasonable suspicion or probable cause.<sup>58</sup> In the Court’s words, the border search cases “reflect longstanding concern for the protection of the integrity of the border.”<sup>59</sup> And, in this case, the concern was heightened by the “national crisis” caused by the smuggling of illegal narcotics.<sup>60</sup> For these reasons, the detention was permissible given that reasonable suspicion was present.

---

<sup>51</sup> Id at 541.

<sup>52</sup> *Montoya de Hernandez*, 473 US at 534–36.

<sup>53</sup> See id at 541 & n 4.

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

<sup>55</sup> See *Montoya de Hernandez*, 473 US at 537.

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

<sup>57</sup> *Montoya de Hernandez*, 473 US at 538–40.

<sup>58</sup> See id.

<sup>59</sup> Id at 538.

<sup>60</sup> Id.

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

These dissenting justices drew a distinction that is, in some ways, parallel to limiting conditions that the Court has recognized in other lines of search cases that include exceptions to the warrant requirement. In *Arizona v Gant*,<sup>64</sup> the Court held that a vehicle search incident to arrest was proper only to the extent that it protected officer safety or was likely to produce “evidence relevant to the crime of arrest.”<sup>65</sup> 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.<sup>66</sup> Brennan could be seen as advocating for a similar standard in the border search context, requiring that the border search exception be tightly tethered to the aims of the border search doctrine: controlling “who and what may enter the country.”<sup>67</sup>

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

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

---

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

<sup>62</sup> Id at 549 (Brennan dissenting).

<sup>63</sup> Id at 554 (Brennan dissenting) (emphasis and citations omitted).

<sup>64</sup> 556 US 332 (2009).

<sup>65</sup> Id at 343–44.

<sup>66</sup> *Edmond*, 531 US at 47.

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

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

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

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

---

<sup>68</sup> See *Flores-Montano*, 541 US at 152.

<sup>69</sup> Id at 151–52.

<sup>70</sup> Id at 152.

<sup>71</sup> Id.

<sup>72</sup> *Flores-Montano*, 541 US at 154.

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

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

<sup>75</sup> *Flores-Montano*, 541 US at 154.

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

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

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

The question in the wake of *Flores-Montano* is whether the “dignity and privacy interests of the person being searched” ever require limitations on searches of property.<sup>80</sup> 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.<sup>81</sup> Lower court judges trying to apply *Flores-Montano* to searches of electronic devices have differed on this point.<sup>82</sup>

## II. BORDER SEARCHES AND ELECTRONIC DEVICES

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

---

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

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

<sup>79</sup> See *id.* at 155–56.

<sup>80</sup> *Id.* at 152.

<sup>81</sup> See *id.*

<sup>82</sup> See notes 118–22 and accompanying text.

<sup>83</sup> See *Flores-Montano*, 541 US at 155–56.

<sup>84</sup> See notes 115–16 and accompanying text.

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

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

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

---

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

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

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

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

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

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

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

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.'" <sup>95</sup> The court saw no reason why searches of electronic devices were less expected than any other type of search.

---

<sup>89</sup> See notes 52–54 and accompanying text.

<sup>90</sup> 393 F3d 501 (4th Cir 2005).

<sup>91</sup> See *id.* at 505.

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

<sup>93</sup> See *Ickes*, 393 F3d at 505–07.

<sup>94</sup> See *id.* at 506–07.

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

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

Importantly, there was no question in the *Ickes* case that reasonable suspicion was present. A routine search of Ickes’s car at the border revealed “marijuana seeds, marijuana pipes, and a copy of a Virginia warrant for Ickes’s arrest. [The officers] also found several albums containing photographs of provocatively posed prepubescent boys, most nude or semi-nude.”<sup>98</sup> This alone would normally raise at least reasonable suspicion that child pornography would be present on Ickes’s electronic devices.<sup>99</sup> 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.”<sup>100</sup> Though this case establishes that reasonable suspicion is not needed for the search of laptops and other electronic devices in the course of a border search, the agents in this case had not only reasonable suspicion and probable cause, but a freely given confession.

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

---

<sup>96</sup> *Ickes*, 393 F3d at 507.

<sup>97</sup> See *id.*

<sup>98</sup> *Id.* at 503.

<sup>99</sup> *Id.* at 507.

<sup>100</sup> *Ickes*, 393 F3d at 503.

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

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

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

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

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

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.<sup>105</sup> 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*,<sup>106</sup> the agent began with a cursory examination of Arnold's laptop. “When the computer had booted up, its desktop displayed numerous icons and folders. Two folders were entitled ‘Kodak Pictures’ and one was entitled ‘Kodak Memories.’ [The agents] clicked on the Kodak folders, opened the files, and viewed the photos on Arnold's computer including one that depicted two nude women.”<sup>107</sup> Though the government did not argue that these pictures depicted minors,<sup>108</sup> Arnold was nevertheless detained for several hours as his laptop was searched. The agents eventually found child pornography.<sup>109</sup>

---

<sup>103</sup> Id at 506–07.

<sup>104</sup> Id at 507.

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

<sup>106</sup> 533 F3d 1003 (9th Cir 2008).

<sup>107</sup> Id at 1005.

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

<sup>109</sup> *Arnold*, 533 F3d at 1005.

Though the Ninth Circuit would later adopt some measure of protection against laptop searches,<sup>110</sup> in this case it followed the Fourth Circuit's example, holding that the search did not require reasonable suspicion.<sup>111</sup> Foreshadowing the questions it would address in *Cotterman*,<sup>112</sup> 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."<sup>113</sup> The defendant in *Arnold* attempted to analogize laptops to homes, particularly citing the number of personal documents likely to be stored on them and the number of secrets that could be revealed by searching them.<sup>114</sup> 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."<sup>115</sup> Though laptops may contain substantial personal and expressive material, the court saw no reason to differentiate their search from any of the other searches that the Ninth Circuit had previously approved absent reasonable suspicion. These permissible searches included: "(1) the contents of a traveler's briefcase and luggage; (2) a traveler's 'purse, wallet, or pockets'; (3) papers found in containers such as pockets (allowing search without particularized suspicion of papers found in a shirt pocket); and (4) pictures, films and other graphic materials."<sup>116</sup>

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*.<sup>117</sup> 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."<sup>118</sup> But neither exception applied here: the behavior of the customs agents

---

<sup>110</sup> See Part II.C.

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

<sup>112</sup> See Part II.C.

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

<sup>114</sup> See *Arnold*, 533 F3d at 1006.

<sup>115</sup> *Id.* at 1007.

<sup>116</sup> *Id.* (citations omitted).

<sup>117</sup> See Part I.C.

<sup>118</sup> *Arnold*, 533 F3d at 1008–09.

appeared to have been professional, and the laptop itself was undamaged.<sup>119</sup>

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

### C. The Ninth Circuit, Revisited

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

---

<sup>119</sup> See *id.*

<sup>120</sup> *Flores-Montano*, 541 US at 154–56.

<sup>121</sup> See Part III.D.1.

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

<sup>123</sup> *Cotterman*, 709 F3d at 956.

<sup>124</sup> *Id.* at 957.

<sup>125</sup> See *id.* at 957–58.

<sup>126</sup> *Id.*

<sup>127</sup> *Cotterman*, 709 F3d at 958.

<sup>128</sup> *Id.*

<sup>129</sup> *Id.*

<sup>130</sup> *Id.* at 959.

reasonable suspicion and whether reasonable suspicion was present.<sup>131</sup>

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.'" <sup>132</sup> Citing *Flores-Montano*, it emphasized the need to consider the "dignity and privacy interests of the person being searched," as well as the problems with searches of property that are destructive, particularly offensive, or overly intrusive as carried out.<sup>133</sup> Despite drawing on the same case law as the prior decisions, this choice of focus presented a starkly different picture of the border search doctrine.

The Ninth Circuit then adopted much the same reasoning that it had rejected in *Arnold*. It stated that a laptop search "directly implicat[es] substantial personal privacy interests. The private information individuals store on digital devices—their personal 'papers' in the words of the Constitution—stands in stark contrast to the generic and impersonal contents of a gas tank."<sup>134</sup> 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."<sup>135</sup>

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."<sup>136</sup> As in *Ickes*,<sup>137</sup> the court here made an empirical claim about what ordinary people expect and assigned legal significance to its assumptions.

---

<sup>131</sup> See *Cotterman*, 709 F3d at 957.

<sup>132</sup> Id at 960, quoting *Montoya de Hernandez*, 473 US at 539.

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

<sup>134</sup> *Cotterman*, 709 F3d at 964.

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

<sup>136</sup> *Cotterman*, 709 F3d at 967.

<sup>137</sup> See *Ickes*, 393 F3d at 506–07.

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

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

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

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

---

<sup>138</sup> *Cotterman*, 709 F3d at 960.

<sup>139</sup> *Id* at 962.

<sup>140</sup> *Id* at 962–63.

<sup>141</sup> *Id* at 957.

<sup>142</sup> *Cotterman*, 709 F3d at 966.

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

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

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

and effects.<sup>146</sup> In the eyes of the majority, this extensive border search eviscerated the target's privacy interests.<sup>147</sup>

1. Adapting doctrine to account for changes in technology.

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

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

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

---

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

<sup>147</sup> See *Cotterman*, 709 F3d at 957.

<sup>148</sup> See *id.* at 956–57.

<sup>149</sup> 533 US 27 (2001).

<sup>150</sup> *Id.* at 40.

<sup>151</sup> See *Cotterman*, 709 F3d at 965.

<sup>152</sup> See *id.* at 964.

<sup>153</sup> See *id.* at 965.

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

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

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

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

---

<sup>154</sup> Id at 964.

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

<sup>156</sup> *Riley*, No 13-132, slip op at 21.

<sup>157</sup> *Cotterman*, 709 F3d at 965.

<sup>158</sup> See id.

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

upon personal privacy and dignity,” the *Cotterman* court held that a showing of reasonable suspicion was necessary in the context of forensic examinations of computers, calling it “a modest requirement in light of the Fourth Amendment.”<sup>160</sup>

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

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

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

---

<sup>160</sup> *Cotterman*, 709 F3d at 968.

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

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

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

<sup>164</sup> *Cotterman*, 709 F3d at 982 (Smith dissenting).

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

Both Smith and Callahan also specifically rejected the argument that the quantity of data stored in electronic devices should change the analysis. According to Smith, “The documents carried on today’s smart phones and laptops are different only in form, but not in substance, from yesterday’s papers, carried in briefcases and wallets.”<sup>167</sup> 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.”<sup>168</sup> The majority argued that size mattered, increasing the magnitude of the privacy invasion, but Callahan and Smith saw no basis in the doctrine for that conclusion.<sup>169</sup>

#### 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.<sup>170</sup> Some courts have explicitly held reasonable suspicion irrelevant to the more routine computer

---

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

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

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

<sup>168</sup> *Cotterman*, 709 F3d at 987 (Smith dissenting) (emphasis omitted).

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

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

searches at issue in particular cases.<sup>171</sup> Others have found reasonable suspicion and not determined whether it was necessary.<sup>172</sup>

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.<sup>173</sup> A more extensive and much-anticipated opinion in *Abidor v Napolitano*<sup>174</sup> reached a similar result, holding that reasonable suspicion was present, rendering moot the question whether it was required.<sup>175</sup> That case concerned a challenge to Department of Homeland Security directives that authorize the search of electronic devices at border crossings.<sup>176</sup> In reaching its conclusion, the court emphasized that travelers know that their electronic devices are at risk of both search and theft and therefore would be wise to choose carefully what files they carry with them.<sup>177</sup>

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

---

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

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

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

<sup>174</sup> 2013 WL 6912654 (EDNY).

<sup>175</sup> See id at \*18.

<sup>176</sup> Id at \*1.

<sup>177</sup> See id at \*13–14.

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

### III. AN EMPIRICAL STUDY OF LAY ATTITUDES AND EXPECTATIONS

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

#### A. Past Work on the Perceived Intrusiveness of Searches

There is a limited amount of prior empirical work analyzing privacy attitudes in the context of police searches, much of it by Professors Christopher Slobogin and Joseph Schumacher. In the early 1990s, Slobogin and Schumacher conducted a survey asking a sample of students to rate the perceived intrusiveness of various types of searches drawn from controversial Fourth Amendment cases.<sup>182</sup> 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

---

<sup>179</sup> See *Flores-Montano*, 541 US at 152.

<sup>180</sup> See notes 85–87 and accompanying text.

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

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

phone for thirty days were seen as only slightly less intrusive.<sup>183</sup> 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.<sup>184</sup>

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

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

---

<sup>183</sup> See id at 738–39.

<sup>184</sup> See id.

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

<sup>186</sup> See id at 359.

<sup>187</sup> See text accompanying notes 53–54.

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

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

the status quo. The more intrusive something is, the more it alters the world that existed before. As a result, police techniques that are common, are expected, or go unnoticed will tend to seem unintrusive.”<sup>190</sup> Similarly, that which is uncommon or unexpected will seem more intrusive. But merely because something is uncommon does not mean that it violates civil liberties (and merely because it is common does not mean that it does not).<sup>191</sup> 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.<sup>192</sup> The resulting set of respondents was diverse, if not representatively weighted. Ten participants were excluded for having completion times that were less than half that of the median participant, and a further five were eliminated because they reported that they were not US citizens, leaving 285 participants. Of the remaining sample, the median age was 35 (range 18–74,  $M = 37.56$ ,  $SD = 12.77$ ). 54.7 percent of the sample was female, 46.7 percent held a valid passport, and 71.6 percent had traveled outside the United States at some point. According to the State Department, in 2013 there were 117.4 million passports in circulation for 316.1 million Americans (37.2 percent),<sup>193</sup> making the sample more travel ready than the national population as a whole. The sample was also somewhat better educated, with a greater proportion of participants holding four-year college degrees.<sup>194</sup> 85.6 percent of

---

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

<sup>191</sup> See id at 959.

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

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

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

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

### C. Types of Searches

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

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

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

---

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

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

2014]

*Searching Electronic Devices at the Border*

1193

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

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

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

#### D. Procedures and Results

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

---

<sup>196</sup> Other than the preamble, this is the same prompt as before.

Whether they are a citizen returning from abroad or a tourist from another country, a person can be searched when they cross the border into the United States. . . . Some [search] methods can be used on any traveler, regardless of whether they have done anything to make the border guards suspicious. Others can only be used if the traveler seems shift 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*.<sup>197</sup> The final question for each search asked participants whether the government could conduct this search on “any traveler they choose,” “[o]nly if they can give a particular reason to suspect the specific traveler of criminal activity” (intended to capture the meaning of reasonable suspicion), or “[o]nly if they have a warrant from a judge.”<sup>198</sup>

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.<sup>199</sup> The results are presented in Table 1. The most severe of the electronic searches are seen as nearly as intrusive as body cavity and strip searches. Five electronic searches, including the forensic analysis from *Cotterman* and the reading of an entire text message archive, are seen as significantly more intrusive than all of the traditional searches other than those two body searches. Every electronic search that

---

<sup>197</sup> See *Flores-Montano*, 541 US at 152.

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

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

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

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

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

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

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

---

<sup>200</sup> See *Cotterman*, 709 F3d at 987 (Smith dissenting).

<sup>201</sup> See *Flores-Montano*, 541 US at 155–56.

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

<sup>203</sup> Compare *Cotterman*, 709 F3d at 967, with *Ickes*, 393 F3d at 506.

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

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

2014]

*Searching Electronic Devices at the Border*

1197

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

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

N = 285

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

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

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

## 2. Extent of revelation.

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

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

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

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

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

### 3. Correlates of privacy concern.

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

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

---

<sup>204</sup> For the sample’s distributions on these, see text accompanying notes 192–93.

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

<sup>206</sup> See id at \*13.

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

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

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

---

<sup>207</sup> The lowest value in the high-severity category was 68 percent and the highest in the low-severity category was 38 percent.

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

---

<sup>208</sup> 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.

2014]

*Searching Electronic Devices at the Border*

1203

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

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

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

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

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

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

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

#### 4. Differences among types of participants.

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

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

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

TABLE 5. DIFFERENCES BASED ON EXTENT OF PRIOR TRAVEL EXPERIENCE

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

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

It could be that travelers have become hardened to the low-severity searches from frequent exposure. In contrast, travelers almost never experience the electronic searches,<sup>209</sup> 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

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

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

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

#### IV. APPLYING THE RESULTS TO POLICY

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

---

<sup>210</sup> See Kerr, 107 Mich L Rev at 958 (cited in note 190) (discussing the meaning of intrusiveness).

<sup>211</sup> *Smith v Maryland*, 442 US 735, 740 n 5 (1979).

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

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

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

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

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

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

---

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

<sup>216</sup> *Id* at 508.

<sup>217</sup> *Id* at 512.

<sup>218</sup> See *id* at 522–23.

<sup>219</sup> *Flores-Montano*, 541 US at 152.

<sup>220</sup> See *Montoya de Hernandez*, 473 US at 541 n 4.

<sup>221</sup> See Part III.D.1.

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

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

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

Since substantial privacy interests are implicated in searches of electronic devices, it is worth reconsidering the purposes underlying the government’s countervailing interest in extensive border searches. The doctrine was created to control “who and what may enter the country.”<sup>224</sup> 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.<sup>225</sup> 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.<sup>226</sup> An officer conducting

---

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

<sup>223</sup> See id at 178–79.

<sup>224</sup> *Ramsey*, 431 US at 620.

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

<sup>226</sup> See *Terry*, 392 US at 26.

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

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

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

## CONCLUSION

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

---

<sup>227</sup> Id at 27.

<sup>228</sup> See *House v Napolitano*, 2012 WL 1038816, \*2 (D Mass).

<sup>229</sup> Id.

<sup>230</sup> Id at \*3.

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

<sup>232</sup> See *Ramsey*, 431 US at 620.

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

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

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

---

<sup>233</sup> 116 US 616 (1886).

<sup>234</sup> See *id.* at 631–32 (stating that compelling the production of private papers “cannot abide the pure atmosphere of political liberty and personal freedom”).