AMERICAN CONSTITUTION SOCIETY

Issue Brief September 2019

Protecting Digital Data at the U.S. Border

By Sophia Cope*

Most of us have electronic devices such as cell phones, laptops, tablets, or other devices that we carry with us frequently, even every day—including when we travel internationally.[1] But do you expect that U.S. government agents, without court authorization and often without any suspicion of wrongdoing, will look through everything on those devices just because you crossed the border? The answer is probably "no."

But that is exactly what is happening—egregious invasions of personal privacy by border agents, who have virtually unfettered access to the private lives of Americans and others entering the U.S. at ports of entry such as international airports and land checkpoints.[2] And the problem is only getting worse. U.S. Customs and Border Protection (CBP) conducted 33,295 electronic device searches in fiscal year 2018.[3] This is compared to 5,085 searches for fiscal year 2012—reflecting an over six-fold increase in six years.[4]

Moreover, it is not the case that only bad actors are being targeted for invasive electronic device searches at the border. Innocent people from all walks of life have been singled out.[5] They

---

* See all of EFF's border search work at *Border Searches*, ELEC. FRONTIER FOUND. (last visited Apr. 12, 2019).

[1] 96% of Americans own a cell phone and 81% own a smartphone. *Mobile Fact Sheet*, PEW RESEARCH CTR. (June 12, 2019).

[2] The border includes 328 land, air, and seaports of entry. *See Border Security: At Ports of Entry*, U.S. CUSTOMS AND BORDER PROT. (last updated Apr. 2, 2018).

[3] *See* Plaintiffs' Statement of Undisputed Material Facts In Support of Their Motion for Summary Judgment at ¶ 52, Alasaad v. McAleenan , No. 17-cv-11730-DJC (D. Mass. Apr. 30, 2018), ECF No. 90-2.

[4] Sophia Cope, *Deep Dive: DHS and CBP Nominees' Unsatisfying Responses to Senators' Questions on Border Device Searches*, ELEC. FRONTIER FOUND. (Dec. 1, 2017).

[5] *See, e.g.*, *Alasaad v. McAleenan: Plaintiffs' Stories*, ELEC. FRONTIER FOUND. (last visited Apr. 12, 2019).

include lawyers[6] and journalists[7], who have unique interests in maintaining the confidentiality of their communications and professional work product. At a moment when lawyers are providing critical counsel to migrants on both sides of the U.S.-Mexico border, and journalists have been covering the unfolding crisis, this practice is particularly troubling.[8]

There is longstanding Supreme Court jurisprudence permitting border agents to conduct warrantless and often suspicionless searches of personal property such as luggage and vehicles without violating the Fourth Amendment. However, the federal agencies charged with border security have interpreted this precedent—the so-called "border search exception" to the Fourth Amendment's warrant and probable cause requirements—as applying to electronic devices like cell phones and laptops.[9]

CBP's current policy, adopted in 2018, creates a distinction between "basic" and "advanced" border device searches.[10] Basic searches (i.e., *manually* searching a device by tapping or mousing around the device to open applications or files) may be conducted without suspicion.[11] Advanced searches (i.e., using other devices or software to conduct a *forensic* analysis[12] of the contents of a device) require reasonable suspicion[13] of activity in violation of the laws enforced

---

[6] *See* Letter from Linda Klein, President, Am. Bar Ass'n, to Gen. John F. Kelly, Sec'y of Homeland Sec. (May 5, 2017).

[7] *Nothing to Declare: Why U.S. Border Agency's Vast Stop and Search Powers Undermine Press Freedom*, COMM. TO PROTECT JOURNALISTS (Oct. 22, 2018).

[8] *See* Tom Jones, Mari Payton, & Bill Feather, *Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database*, NBC7 SAN DIEGO (Mar. 6, 2019).

[9] The U.S. Department of Homeland Security (DHS) is responsible for border security. Two of its component agencies process and investigate travelers to and from the United States: U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE). CBP officers are the frontline agents that travelers first encounter at ports of entry such as international airports and land checkpoints. CBP officers regularly interview and search travelers and their belongings as they seek to enter (or leave) the country. When CBP officers seize an electronic device at the border, they often turn it over to ICE for forensic analysis by its Homeland Security Investigations (HSI) unit. ICE/HSI officers may also independently initiate border device searches, and they may conduct manual searches. Once ICE officers have possession of a traveler's device, ICE policy is operative and not CBP policy. *See* IMMIGRATION & CUSTOMS ENF'T, DIRECTIVE NO. 7-6.1, BORDER SEARCHES OF ELECTRONIC DEVICES § 6.2 (Aug. 18, 2009) [hereinafter *ICE 2009 Policy*].

[10] U.S. CUSTOMS & BORDER PROT., DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (Jan. 4, 2018) [hereinafter *CBP 2018 Policy*].

[11] *CBP 2018 Policy*, *supra* note 10, § 5.1.3.

[12] While forensic device searches tend to provide efficiencies in analyzing and cataloging data, they generally can access the same information that a manual search can access. A key difference is that forensic searches can sometimes uncover deleted information. *See* United States v. Kolsuz, 185 F. Supp. 3d 843, 849 n.8 (E.D. Va. 2016); United States v. Cotterman, 709 F.3d 952, 958 n.5 (9th Cir. 2013) (en banc).

[13] Reasonable suspicion is a legal standard lower than probable cause but higher than no suspicion. The Ninth Circuit has defined reasonable suspicion, for example, as "a particularized and objective basis for

or administered by CBP[14]—*unless* "there is a national security concern," then reasonable suspicion is not needed for an advanced search.[15] This "national security" exception can be construed exceedingly broadly and CBP has provided few standards for border agents to follow.[16] Civil liberties advocates worry that this national security exception creates a loophole that is large enough to swallow the reasonable suspicion rule.

U.S. Immigration and Customs Enforcement's (ICE) public-facing policy, adopted in 2009, permits warrantless and suspicionless border device searches.[17] However, ICE has asserted in litigation that it now also makes a distinction between methods of search, where "basic" device searches require no suspicion and "advanced" device searches require reasonable suspicion; though ICE has not adopted a national security exception for advanced searches.[18]

While CBP and ICE have interpreted their border search authority broadly, the Supreme Court has yet to answer the question of whether electronic devices properly fall under the border search exception. As this Issue Brief will argue, digital is different. Given the unprecedented and significant privacy interests travelers have in their electronic devices, and the government's weak interests in obtaining virtually unfettered access to the highly personal digital data they contain, it is unreasonable to apply the border search exception to electronic devices. U.S. border agents should have to get a warrant before searching digital data travelers carry across the border.

I. The Border Search Exception

Under the current conception of the Fourth Amendment, government agents at the U.S. border generally enjoy more power than police officers working in the interior of the country. Most of the time, border agents exercise these powers against travelers arriving to the United States, but they sometimes apply them to travelers leaving the country as well.[19]

However, the U.S. border is not a Constitution-free zone. The powers of border agents are tempered by our First Amendment rights to speak and associate privately and to gather the news, our Fifth Amendment right to freedom from self-incrimination, and, most importantly for this Issue Brief, our Fourth Amendment right to privacy.

---

suspecting the particular person stopped of criminal activity. This assessment is to be made in light of the totality of the circumstances." *Cotterman*, 709 F.3d at 968 (internal quotes and citations omitted).

[14] CBP is authorized to enforce numerous laws. *See Summary of Laws Enforced by CBP*, U.S. CUSTOMS & BORDER PROT. (last visited Apr. 12, 2019).

[15] *CBP 2018 Policy*, *supra* note 10, § 5.1.4.

[16] The 2018 policy references individuals on terrorist watchlists, but then mentions unspecified "other articulable factors as appropriate." *Id.*

[17] *ICE 2009 Policy*, *supra* note 9, § 6.1.

[18] *See supra* note 3, at ¶¶ 17-19.

[19] *CBP 2018 Policy*, *supra* note 10, § 4; *ICE 2009 Policy*, *supra* note 9, § 4.

The Fourth Amendment prohibits "unreasonable" searches and seizures by the government.[20] The default rule to ensure that a search or seizure is reasonable is that law enforcement officials must first obtain a probable cause warrant.[21] This means that the police officer must present preliminary evidence under oath to a judge that shows that the thing to be searched or seized likely contains evidence of illegal activity. The judge, if convinced that there is probable cause, will then issue an order authorizing the search or seizure.

The Supreme Court has ruled that exceptions to the warrant and probable cause requirements may only be justified when legitimate governmental interests outweigh individual privacy interests.[22] Suspicionless searches, in particular, have been justified when the "primary purpose"[23] of a search is "beyond the normal need for law enforcement"[24] or "beyond the general interest in crime control."[25] Crucially, warrantless, suspicionless searches in a particular context must be "tethered" to the purposes or rationales justifying the exception.[26]

The Supreme Court has interpreted the Fourth Amendment to include a categorical "border search exception" to the standard warrant and probable cause requirements (though, importantly, not the reasonableness requirement). In fact, the Court has permitted wholly suspicionless "routine" searches—a term the Court has only partially defined—of luggage and other common possessions presented at the border. Thus, the border search exception provides that border searches never require a judicial warrant and, in the case of "routine" border searches, any individualized suspicion that the personal property to be searched contains evidence of illegal activity.[27]

The Supreme Court has justified the border search exception by reasoning that travelers have minimal privacy interests in their luggage because they are unlikely to carry highly personal information in their suitcases and other bags, and that any privacy interests that do exist in travelers' bags are outweighed by legitimate governmental interests.

---

[20] U.S. CONST. amend. IV, cl. 1. *See also* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("the ultimate touchstone of the Fourth Amendment is 'reasonableness.'").
[21] *See* Katz v. United States, 389 U.S. 347, 357 (1967) (noting warrantless searches "are per se unreasonable").
[22] Riley v. California, 573 U.S. 373, 385 (2014) (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
[23] City of Indianapolis v. Edmond, 531 U.S. 32, 48 (2000).
[24] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).
[25] *City of Indianapolis*, 531 U.S. at 48. *Cf. Riley*, 573 U.S. at 382 (citing *Vernonia School District 47J*, 515 U.S. at 653 ("[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant.")).
[26] *Riley*, 573 U.S. at 386 (citing Arizona v. Gant, 556 U.S. 332, 343 (2009)). *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").
[27] United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

The government's interest in protecting the "integrity of the border"[28] is justified by two narrow purposes: immigration and customs enforcement.[29] Thus, the Supreme Court has presumed that warrantless, suspicionless border searches are critical to: (1) ensuring that travelers entering the U.S. have proper authorization and documentation and would not be harmful to U.S. interests; and (2) enforcing the laws regulating the importation of goods into (or exportation from) the U.S., including duty requirements, and preventing the entry of harmful items such as drugs, weapons, and infested agricultural products.[30]

Given that the Fourth Amendment's border search exception developed in the pre-digital era, and electronic devices contain extraordinary amounts of highly personal information, it is unreasonable to apply the Fourth Amendment's border search exception to modern electronic devices. Two strands of Fourth Amendment jurisprudence support the conclusion that border agents should have to obtain a probable cause warrant before they search travelers' electronic devices: 1) border search case law itself, which contemplates that some border searches may be "non-routine;" and 2) the balancing test the Supreme Court applies to determine whether a new type of property should fall under an existing categorical exception to the Fourth Amendment's warrant and probable cause requirements, which the Court most recently applied in *Riley v. California*.

II. Border Searches of Electronic Devices Should Require a Warrant Because They Are "Non-Routine"

Supreme Court border search jurisprudence recognizes that not all border searches are "routine." Some border searches are "highly intrusive" and impact the "dignity and privacy interests" of individuals,[31] or are carried out in a "particularly offensive manner."[32] Such "non-routine" border searches require that border agents have "reasonable suspicion" about the traveler, specifically, that there is reasonable cause to believe they are in violation of an

---

[28] *Id.* at 538.

[29] United States v. Cotterman, 709 F.3d 952, 956 (9th Cir. 2013) (en banc) (discussing the "narrow border search exception").

[30] *See, e.g.*, Boyd v. United States, 116 U.S. 616, 623 (1886) (power to identify "goods liable to duties and concealed to avoid the payment thereof," but not for "seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him"); Carroll v. United States, 267 U.S. 132, 154 (1925) (power to require a traveler "to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in"); Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) (power to exclude aliens); United States v. Ramsey, 431 U.S. 606, 620 (1977) (power "to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country"); *Montoya de Hernandez*, 473 U.S. at 537, 544 (power "to regulate the collection of duties and to prevent the introduction of contraband" or "anything harmful" such as "communicable diseases, narcotics, or explosives").

[31] United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

[32] *Id.* at 154 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13).

immigration or customs law.[33] Thus, for example, the Supreme Court held that disassembling a gas tank, without permanently damaging it, at the border is a "routine" search that may be conducted without a warrant or even any individualized suspicion.[34] However, detaining a traveler at the border until they have defecated to see if they are smuggling drugs in their digestive tract is a "non-routine" seizure and search that requires "reasonable suspicion" that the traveler is a drug mule.[35]

The U.S. Court of Appeals for the Ninth Circuit was the first appellate court to hold that certain border searches of electronic devices are "non-routine." In *U.S. v. Cotterman* (2013), the Ninth Circuit held that border agents needed reasonable suspicion before they could conduct a *forensic* search, aided by sophisticated software, of the defendant's laptop. Unfortunately, the court also held that a *manual* search of an electronic device is "routine" and so a warrantless, suspicionless manual border device search is reasonable under the Fourth Amendment.[36]

While a rule categorizing as "non-routine" forensic border searches of electronic devices is an improvement over prior precedent, *all* border searches of electronic devices should be considered "non-routine" regardless of the search method used by border agents. There is no valid distinction between manual and forensic searches, because both are extraordinarily invasive of travelers' privacy by accessing essentially the same trove of highly personal information.[37] Any border search of an electronic device—whether conducted manually or with specialized forensic tools—is "non-routine" because it is a "highly intrusive" search that implicates the "dignity and privacy interests" of the traveler, or may be considered "particularly offensive."[38]

Assuming all border searches of electronic devices are "non-routine," it does not follow that reasonable suspicion is the highest standard that may apply. The Supreme Court's border search decisions establish reasonable suspicion as the *floor* for highly intrusive searches. The Court has never suggested that reasonable suspicion is the ceiling for every border search, or that property searches can never require heightened protection.[39]

Therefore, given that travelers have unprecedented and significant privacy interests in their digital data, border searches of electronic devices should not only be considered highly

---

[33] *See supra* note 13.
[34] *Flores-Montano*, 541 U.S. at 155.
[35] *Montoya de Hernandez*, 473 U.S. at 541.
[36] United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (en banc).
[37] *See supra* note 12.
[38] *See Flores-Montano*, 541 U.S. at 152.
[39] *See Montoya de Hernandez*, 473 U.S. at 541 n.4 ("[T]oday we suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches."); *Flores-Montano*, 541 U.S. at 152; House v. Napolitano, 2012 WL 1038816, at *7 (D. Mass. 2012) (noting the "Supreme Court has not explicitly held that all property searches" never require suspicion).

intrusive "non-routine" searches, they should also require a probable cause warrant under the Supreme Court's existing border search jurisprudence.

III. Border Searches of Electronic Devices Should Require a Warrant Because the *Riley* Balancing Test Favors the Privacy Interests of the Traveler

The Supreme Court in *Riley v. California* reiterated that in determining whether to apply an existing warrant exception to a "particular category of effects"—such as cell phones—the Fourth Amendment requires that individual privacy interests be balanced against legitimate governmental interests.[40] In the case of border searches of electronic devices, this balancing clearly favors the traveler. Thus, the border search exception should not apply to electronic devices, and border agents should first obtain a probable cause warrant.

A. The *Riley* Balancing Test

In *Riley*, the Supreme Court held that cell phones do not fall within the search-incident-to-arrest exception, which generally permits police officers to conduct warrantless, suspicionless searches of arrestees and items on their persons. The Court concluded that arrestees' privacy interests in the digital data their cell phones contain outweigh governmental interests. Thus, police officers must obtain a probable cause warrant to search the cell phone of an arrestee.[41]

First, in examining individual privacy interests, the *Riley* Court considered the nature of cell phones themselves—rather than how the devices are searched, in contrast to *Cotterman*.[42] The Court recognized that cell phones are unlike any other physical containers, given their "immense storage capacity" and the "highly personal" nature of the information they contain.[43] The Court rejected the government's argument that cell phones are the same as physical items: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon" just because both are "ways of getting from point A to point B."[44] The Court continued: "Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[45]

The *Riley* Court stressed the significant privacy interests in the vast amounts of highly personal information modern cell phones contain—call logs, emails, text messages, voicemails, browsing history, calendar entries, contact lists, shopping lists, notes, photos and videos, geolocation logs, and other personal files. And that information can reveal an individual's political affiliations,

---

[40] *Riley*, 573 U.S. at 386.
[41] *Id.* at 386.
[42] It is worth noting that the unlawful warrantless cell phone searches in *Riley* were conducted manually. *Id.* at 379.
[43] *Id.* at 393-395.
[44] *Id.* at 393.
[45] *Id.*

religious beliefs and practices, sexual and romantic lives, financial status, health conditions, and family and professional associations. This is compounded by the fact that cell phones and other electronic devices can cover many years of a person's life.[46] Indeed, because cell phones can in fact reveal the "sum of an individual's private life," the *Riley* Court recognized that any search by the government is an unprecedented intrusion into individual privacy.[47]

Second, the government's interests are analyzed by considering whether warrantless, suspicionless searches of the particular type of personal property at issue are sufficiently "tethered" to the purposes or rationales justifying the exception sought to be applied.[48]

The *Riley* Court concluded that the tethering or nexus is weak between warrantless, suspicionless access to arrestees' cell phones and the two narrow purposes of the search-incident-to-arrest exception: 1) to protect officers from an arrestee who might use a weapon against them, and 2) to prevent the destruction of evidence.[49] That is, warrantless, suspicionless searches of arrestees' cell phones are not necessary to and do not sufficiently advance these goals.[50]

The *Riley* Court reasoned that 1) "data on the phone can endanger no one," and 2) the probability is small that associates of the arrestee will remotely delete digital data.[51] Regarding the latter concern proffered by the government, the Court concluded that the problem is not "prevalent," and therefore the mere possibility does not justify embodying such a significant privacy intrusion within a categorical rule—that is, permitting a warrantless, suspicionless search of a cell phone *for every arrest*.[52]

B. Applying the *Riley* Balancing Test to the Border Search Context

Although *Riley* was not a border search case, the Fourth Amendment analytical framework the Court applied is relevant to the border search context. Application of the *Riley* balancing test supports the conclusion that electronic devices should not fall under the border search exception, and thus border agents should have to obtain a probable cause warrant before searching electronic devices.

First, the unprecedented and significant privacy interests in cell phones articulated by the *Riley* Court do not change just because a traveler brings a cell phone or other electronic device across

---

[46] *Id.* at 400 ("The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years.").
[47] *Id.* at 394.
[48] *Id.*
[49] *Id.* at 393-394, 387-390.
[50] *See* United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013), *aff'd sub nom. Riley*, 573 U.S. at 386.
[51] *Riley*, 573 U.S. at 387.
[52] *See id.* at 395 ("Allowing the police to scrutinize [personal] records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.").

the U.S. border. Border searches of luggage and other non-digital personal property, like non-digital searches incident to arrest, are "limited by physical realities and tend[] as a general matter to constitute only a narrow intrusion on privacy."[53] By contrast, border searches of electronic devices are highly intrusive and "bear[] little resemblance" to searches of travelers' luggage.[54]

Second, warrantless, suspicionless searches of electronic devices are not sufficiently "tethered" to the narrow purposes justifying the border search exception: immigration and customs enforcement. That is, warrantless, suspicionless border searches of electronic devices are not necessary to and do not sufficiently advance these goals. As with the search-incident-to-arrest exception, the border search exception might "strike[] the appropriate balance in the context of physical objects," but its underlying rationales do not have "much force with respect to digital content on cell phones" or other electronic devices.[55]

Border agents determine travelers' immigration status and authority to enter the United States by questioning travelers and inspecting official documents such as passports and visas. Border agents enforce customs laws by searching travelers' luggage, vehicles, and, if necessary, their persons.[56] Just as the *Riley* Court stated that "data on the phone can endanger no one," physical items that are subject to import duties or considered contraband such as drugs or weapons cannot be hidden in digital data.

Some digital content, such as child pornography, may be considered "digital contraband" to be interdicted at the border.[57] However, this does not justify a *categorical rule* permitting warrantless, suspicionless border searches of electronic devices for every traveler entering or exiting the country. Unlike physical contraband, digital contraband can easily be transported or viewed across borders via the Internet. Thus the government cannot demonstrate that any digital contraband that might be on travelers' devices is a significant or "prevalent" problem *at the border*, or that the ability to conduct a warrantless, suspicionless device search "would make much of a difference" in preventing its importation into the country.[58]

Even assuming that conducting warrantless, suspicionless searches of electronic devices at the border might sometimes advance the government's goals of immigration and customs

---

[53] *Id.* at 375.
[54] *Id.* at 386.
[55] *Id.* at 386 (citing United States v. Robinson, 414 U.S. 218 (1973)).
[56] *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 151 (2004); United States v. Molina-Gomez, 781 F.3d 13, 16-17 (1st Cir. 2015).
[57] *Cf.* United States v. Thirty-Seven Photographs, 402 U.S. 363, 376-77 (1971).
[58] *Riley*, 134 S. Ct. at 389.

enforcement, the extraordinary privacy interests travelers have in the digital data their electronic devices contain outweigh any governmental interests.[59]

It is worth noting that the *Riley* Court rejected requiring reasonable suspicion for cell phone searches incident to arrest. With regard to protecting privacy, the Court stated that such an intermediary standard (between no suspicion and probable cause) would provide "no practical limit at all when it comes to cell phone searches."[60] Additionally, although an appellate court majority opinion has yet to require a probable cause warrant in the border context, the Supreme Court itself has recognized that the search-incident-to-arrest exception at issue in *Riley* is similar to the border search exception.[61]

C. Encouraging Post-*Riley* Developments

Following *Riley*, lower courts have been grappling with the question of what constitutional standards should apply to border searches of electronic devices.[62] Although no majority appellate opinion has so far required a probable cause warrant, some courts and individual judges have applied the *Riley* analytical framework and recognized the extraordinary privacy interests that travelers have in their digital data—and the weak governmental interests in obtaining warrantless, suspicionless access to that data.

A circuit split has developed in the context of criminal appeals. The Fourth Circuit provided heightened protection for forensic border device searches, similar to the Ninth Circuit's pre-*Riley* decision; and the Ninth Circuit further limited the scope of all warrantless, suspicionless border device searches. Meanwhile, the Eleventh Circuit deferred to the government and held that warrantless, suspicionless border device searches do not violate the Fourth Amendment. The Fifth and Seventh Circuits avoided the constitutional issue entirely.

---

[59] CBP has failed to show that forensic or "advanced" border device searches are even effective. The DHS Inspector General wrote, "One area to measure is the number of instances in which information collected from searches resulted in a prosecution or conviction, but according to [CBP Office of Field Operations], it does not track this information." OFFICE OF INSPECTOR GEN., DHS, OIG-19-10, CBP'S SEARCHES OF ELECTRONIC DEVICES AT PORTS OF ENTRY – REDACTED at 9 (2018).

[60] *Riley*, 573 U.S. at 399.

[61] Prior to *Riley*, the Supreme Court noted the similarity between the border search exception and the search-incident-to-arrest exception. *See* United States v. Ramsey, 431 U.S. 606, 621 (1977).

[62] The Supreme Court's decision in *Carpenter v. United States* also informs the border context. In that case, the Court held that the government must obtain a probable cause warrant for historical cell phone location information maintained by cell phone service providers. The *Carpenter* Court cited *Riley* extensively in examining the significant privacy interests that individuals have in a record of their physical movements. Historical location information can also be obtained from a border search of a cell phone. Citing *Riley*, the *Carpenter* Court stated, "When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents." Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018). Similarly, the border search exception should not be extended to electronic devices.

Additionally, the Electronic Frontier Foundation and the ACLU are currently litigating the first civil case post-*Riley*—*Alasaad v. McAleenan*—to challenge warrantless, suspicionless border searches of electronic devices in Massachusetts District Court.[63]

1. Ninth Circuit

In a decision that came down a year before *Riley*, the Ninth Circuit sitting en banc ruled in *U.S. v. Cotterman* (2013) that a forensic border search of a laptop is a "non-routine" search that requires reasonable suspicion, while a manual search is "routine" and so requires no individualized suspicion of wrongdoing. Similar to *Riley*, however, the *Cotterman* court acknowledged the unique privacy interests that travelers have in the digital data their electronic devices contain. The court distinguished electronic devices from luggage, stating that they "contain the most intimate details of our lives."[64]

In *U.S. v. Cano* (2019), a three-judge panel of the Ninth Circuit unsurprisingly reaffirmed *Cotterman*'s en banc rule and held that a forensic border search of a cell phone requires reasonable suspicion, while a manual search requires no suspicion.[65]

The *Cano* court, however, significantly circumscribed the scope of border device searches, further holding that warrantless, suspicionless border device searches—both manual and forensic—are only permissible under the Fourth Amendment to determine whether the device contains *digital contraband*.[66] The *Cano* court emphasized that border agents may not conduct warrantless, suspicionless border device searches "for evidence of past or future border-related crimes."[67] Additionally, the court held with respect to forensic searches, "We clarify *Cotterman* by holding that 'reasonable suspicion' in this context means that officials must reasonably suspect that the cell phone contains digital contraband."[68]

The *Cano* court did not hold that emails and text messages are totally off limits. The court noted that child pornography may be sent via email or text message, and so border device searches for digital contraband within these kinds of cell phone data are reasonable under the Fourth Amendment.[69] Yet the court also stated that "the detection-of-contraband justification" for

---

[63] Following an encouraging order denying the government's motion to dismiss in 2018, the district court considered summary judgment motions during the summer of 2019. The case will certainly be appealed to the First Circuit, which had considered a case that was consolidated with and affirmed by *Riley*. *See* United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *aff'd sub nom.* Riley v. California, 573 U.S. 373, 386 (2014).
[64] United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (en banc).
[65] United States v. Cano, 2019 WL 3850607, at *2 (9th Cir. 2019).
[66] *Id.*
[67] *Id.* at *10.
[68] *Id.* at *2.
[69] *Id.* at *11.

warrantless, suspicionless border device searches "would rarely seem to apply to an electronic search of a cell phone outside the context of child pornography."[70]

2. Fourth Circuit

After *Riley*, the Fourth Circuit in *U.S. v. Kolsuz* (2018) issued an opinion similar to—and arguably more encouraging than—*Cotterman*. The *Kolsuz* court was the first appellate court post-*Riley* to hold that suspicionless forensic border searches of electronic devices violate the Fourth Amendment.[71] The court acknowledged "the Supreme Court's … decision in *Riley* and its emphasis on the significant privacy interests in the digital contents of phones."[72]

While the *Kolsuz* court declined to hold what the level of suspicion should be, it left open the possibility of a warrant requirement for forensic border device searches.[73] The court also left open the possibility that manual searches may require reasonable suspicion or a warrant, stating, "[w]e have no occasion here to consider whether *Riley* calls into question the permissibility of suspicionless manual searches of digital devices at the border."[74]

3. Fifth Circuit

The Fifth Circuit in *U.S. v. Molina-Isidoro* (2018) avoided the question of whether *Riley* requires a warrant for border device searches and simply concluded that there was probable cause to support the manual search of the defendant's cell phone.[75] However, the majority did emphasize that a leading Fourth Amendment legal treatise recognizes that "*Riley* may prompt a reassessment" of the question.[76]

Additionally, Judge Gregg Costa issued an instructive concurring opinion. In conducting a "tethering" analysis of the government's interests, he considered whether the traditional

---

[70] *Id.* at *12 n.13.

[71] The Fourth Circuit also linked the non-routine doctrine and *Riley*: "We also agree with the district court that under *Riley*, the forensic examination of Kolsuz's phone must be considered a nonroutine border search, requiring some measure of individualized suspicion." United States v. Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018).

[72] *Kolsuz*, 890 F.3d at 140.

[73] *Id.* at 137 ("What precisely that standard should be—whether reasonable suspicion is enough… or whether there must be a warrant based on probable cause… is a question we need not resolve: Because the agents who conducted the search reasonably relied on precedent holding that no warrant was required, suppression of the [cell phone data] would be inappropriate even if we disagreed.").

[74] *Id.* at 146 n. 5.

[75] Similarly, the Seventh Circuit declined to rule on what constitutional standard applies to border searches of electronic devices. The court stated that it "may avoid entirely the thorny issue of the appropriate level of suspicion required. Instead, we affirm the district court's denial of the motion to suppress because these agents acted in good faith when they searched the devices with reasonable suspicion to believe that a crime was being committed . . . ." United States v. Wanjiku, 919 F.3d 472, 479 (7th Cir. 2019).

[76] United States v. Molina-Isidoro, 884 F.3d 287, 292 (5th Cir. 2018).

primary purpose of the border search exception—customs enforcement, including contraband interdiction—justifies conducting warrantless, suspicionless searches of *electronic devices*. Importantly, he concluded that the link between these ends and means is very weak: "Detection of … contraband is the strongest historic rationale for the border search exception." Yet, "[m]ost contraband, the drugs in this case being an example, cannot be stored within the data of a cell phone." He concluded, "this detection-of-contraband justification would not seem to apply to an electronic search of a cellphone or computer."[77]

Judge Costa also questioned whether a new "evidence-gathering justification" could support warrantless, suspicionless border searches of electronic devices. Skeptical of this idea, he cited a 19th Century case about imported goods, *Boyd v. U.S.* (1886), where the Supreme Court had stated,

> The search for and seizure of stolen or forfeited goods, or goods liable to duties and concealed to avoid the payment thereof, are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him.[78]

Judge Costa then stated,

> [*Boyd*'s] emphatic distinction between the sovereign's historic interest in seizing imported contraband and its lesser interest in seizing records revealing unlawful importation has potential ramifications for the application of the border-search authority to electronic data that cannot conceal contraband and that, to a much greater degree than the papers in *Boyd*, contains information that is like an extension of the individual's mind.[79]

4. Eleventh Circuit

The Eleventh Circuit in *U.S. v. Vergara* (2018), which involved a forensic border device search, held that neither a warrant nor probable cause is ever required for a border search, including of an electronic device.[80]

The silver lining is that in *Vergara*, Judge Jill Pryor wrote a thorough dissenting opinion in favor of travelers' constitutional rights. She concluded that "a forensic search of a cell phone at the border requires a warrant supported by probable cause."[81]

---

[77] *Id.* at 295 (Costa, J., concurring).
[78] *Boyd*, 116 U.S. 616,623.
[79] *Molina-Isidoro*, 884 F.3d at 297 (Costa, J., concurring) (internal quotations omitted).
[80] United States v. Vergara, 884 F.3d 1309, 1311 (11th Cir. 2018).
[81] *Id.* at 1313 (Pryor, J., dissenting).

Following the *Riley* balancing test, Judge Pryor acknowledged that travelers' privacy interests in their cell phones are weighty, stating that "cell phones are fundamentally different from any object traditionally subject to government search at the border."[82]

Judge Pryor then found that the government's interests are weak. Similar to Judge Costa of the Fifth Circuit, she determined that the traditional primary rationale underlying the border search exception—contraband interdiction—does not justify conducting warrantless, suspicionless searches of *cell phones*. She stated, "the rationales underlying the border search exception lose force when applied to forensic cell phone searches… [C]ell phones do not contain the physical contraband that border searches traditionally have prevented from crossing the border."[83]

Judge Pryor also dismissed the idea that warrantless cell phone searches are needed to intercept any "electronic contraband." She stated,

> cell phone searches are ill suited to prevent the type of contraband that might be present on a cell phone from entering into the United States. Unlike physical contraband, electronic contraband is borderless and can be accessed and viewed in the United States without ever having crossed a physical border.[84]

Also similar to Judge Costa, Judge Pryor determined that a new "general law enforcement justification" does not support conducting warrantless, suspicionless cell phone searches at the border. She stated that this justification is "quite far removed from the purpose originally underlying the border search exception: 'protecting the Nation from entrants who may bring anything harmful into this country.'"[85] She stated, quoting *Riley*, "[e]xcepting forensic cell phone searches from the warrant requirement because those searches may produce evidence helpful in future criminal investigations would thus 'untether the rule from [its] justifications.'"[86]

5. Massachusetts District Court

Perhaps the most encouraging federal opinion has been that of the U.S. District Court for the District of Massachusetts in the civil case *Alasaad v. McAleenan* (2018). The plaintiffs in *Alasaad* are 10 U.S. citizens and one lawful permanent resident whose electronic devices were searched and/or seized at the border, and who were not subsequently charged with any crimes or other wrongdoing.[87]

---

[82] *Id.* at 1315.
[83] *Id.* at 1317.
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Alasaad v. McAleenan*, ELEC. FRONTIER FOUND. (last visited Apr. 12, 2019).

The judge considered the plaintiffs' argument that a probable cause warrant should be required for border device searches. The judge denied the government's motion to dismiss the case, citing *Riley*. In holding that the "[p]laintiffs have plausibly alleged a Fourth Amendment claim," the judge stated that "digital searches are different . . . since they 'implicate privacy concerns far beyond those implicated' in a typical container search."[88]

IV. A Possible Legislative Solution

In the absence of a directly on-point Supreme Court ruling, or if the Court were to hold that the Constitution does not require a probable cause warrant for border searches of electronic devices, Congress could and should step in.

Over the past two Congresses, two bipartisan bills were introduced to address the problem of border agents accessing with virtually no limits American travelers' electronic devices. During the 116th Congress (2019-2020), Senators Ron Wyden (D-OR) and Rand Paul (R-KY) introduced the Protecting Data at the Border Act (S. 1606/H.R. 2925).[89] In the 115th Congress (2017-2018), Senators Patrick Leahy (D-VT) and Steve Daines (R-MT) introduced a bill (S. 2462), which did not have a formal name.[90]

Both bills only apply to U.S. persons. While it would be preferable if federal legislation circumscribed the device search authority of border agents irrespective of the immigration status of the traveler,[91] both bills would provide meaningful protections for Americans. The key difference between the two bills is that the Wyden-Paul bill creates a warrant requirement across the board while the Leahy-Daines bill does not.

The Protecting Data at the Border Act requires border agents to obtain a judicial warrant based on probable cause before accessing the digital contents of an electronic device in the possession of a U.S. citizen or lawful permanent resident.

By contrast, the Leahy-Daines bill creates separate restrictions based on the type of device search conducted: manual or forensic. For manual searches of electronic devices, the bill requires that border agents have reasonable suspicion that the traveler violated an immigration or customs law and that the electronic device contains evidence relevant to that violation. For forensic searches of electronic devices, the bill requires border agents to obtain a probable cause warrant.

Senators' offices have indicated that they are working on reconciling the two bills.

---

[88] Alasaad v. McAleenan, 2018 WL 2170323, at *20 (D. Mass. 2018) (internal citations omitted).
[89] Protecting Data at the Border Act, S. 1606, 116th Cong. (2019); Protecting Data at the Border Act, H.R. 2925, 116th Cong. (2019).
[90] S. 2462, 115th Cong. (2018).
[91] The United States is a signatory to the International Covenant on Civil and Political rights, which provides, in Article 17, "No one shall be subjected to arbitrary or unlawful interference with his privacy . . . ." G.A. Res. 2200A (XXI), International Covenant on Civil and Political Rights (Dec. 16, 1966).

V. Conclusion

Two strands of Fourth Amendment jurisprudence—border search case law itself related to "non-routine" searches, and the *Riley v. California* balancing test—support the conclusion that the courts should require a probable cause warrant for border searches of electronic devices. In the absence of court action, Congress should step in to protect the rights of travelers. Travelers have extraordinary privacy interests in the digital data their electronic devices contain. Devices like smartphones and laptops reflect a traveler's entire life—and not just at that moment in time, but over many years—and the U.S. government should not have virtually unfettered access to that data. In short, digital is different.

About the Author

Sophia Cope is a Senior Staff Attorney at the Electronic Frontier Foundation (EFF) where she works on a variety of free speech and privacy issues related to the Internet and technology. She has been a civil liberties attorney for 15 years and has experience in both litigation and policy advocacy. Her writing has appeared in *The New York Times*, *The Guardian*, *Slate*, and *Huffington Post*.

Prior to joining EFF, Cope spent eight years in Washington, D.C. She worked at the Newspaper Association of America (now, the News Media Alliance) on freedom of the press and digital media issues. She also worked at the Center for Democracy & Technology on civil liberties and human rights issues related to the Internet and technology. Prior to working in Washington, D.C., she was a litigator at the First Amendment Project in Oakland, California.

Cope was an adjunct professor of media law for nearly four years, teaching at both American University and Shepherd University. She is a graduate of Santa Clara University and University of California, Hastings College of the Law.

About the American Constitution Society

The American Constitution Society (ACS) believes that law should be a force to improve the lives of all people. ACS works for positive change by shaping debate on vitally important legal and constitutional issues through development and promotion of high-impact ideas to opinion leaders and the media; by building networks of lawyers, law students, judges and policymakers dedicated to those ideas; and by countering the activist conservative legal movement that has sought to erode our enduring constitutional values. By bringing together powerful, relevant ideas and passionate, talented people, ACS makes a difference in the constitutional, legal and public policy debates that shape our democracy.