This article has been published in
PLI Current: The Journal of PLI Press, Vol. 2, No. 2,
Spring 2018 (© 2018 Practising Law Institute),
www.pli.edu/PLICurrent.

PLI Current
The Journal of PLI Press
Vol. 2, No. 2, Spring 2018

Privacy Rights Versus National Security at the Border

Rosanna Berardi*

The Basics

The Fourth Amendment provides:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause. . . .[1]

This constitutional requirement operates to protect the privacy interests of the American people, but it is greatly relaxed at the border. That is not to say, however,

* The author would like to thank Angela J. Schnell, Esq. and Zachary Ahlstrom for their assistance in drafting this article.

that the border is a Constitution-free zone. Individual privacy rights still exist, but they are balanced against the United States' interest in self-preservation—a balance struck in favor of the government, as it needs to be.

The border search exception operates as a narrow exception to the Fourth Amendment prohibition against warrantless searches without probable cause. It gives federal agents the power to search every individual crossing the U.S. border. A search of their person and belongings is necessary to ensure the national security of the United States.

Border Search Authority

Border search authority is rooted in "the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country."[2] "Travelers may be stopped 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 lawfully be brought in."[3] In weighing the rights of the individual against national security, national security must triumph to ensure the protection of all. Therefore, border searches are reasonable simply because of their occurrence at the border, as this is when the government's interest in protecting its citizenry from unwanted persons and contraband is highest.[4] Without authority to search, the U.S. Customs and Border Protection would be severely limited in its ability to protect the United States. As border protection is fundamental to a sovereign nation's survival, it stands to reason that the border search exception is a necessary exception to Fourth Amendment protections.

In weighing the rights of the individual against national security, national security must triumph to ensure the protection of all.

Routine and Nonroutine Searches

Federal agents are permitted to search a traveler's person and belongings without a warrant and without suspicion of wrongdoing. In this context, individual privacy rights are limited in favor of national security, so a traveler's expectation of privacy at the border is far lower than it is when inside the United States. This is not to say that Fourth Amendment protections are non-existent at the border.

A "nonroutine" search requires at least a reasonable suspicion of wrongdoing.

While probable cause is never required to search border crossers or their belongings, courts do distinguish between "routine" and "nonroutine" searches, analyzed on a case-by-case basis. A "routine" border search requires no level of suspicion, while a "nonroutine" search requires at least a reasonable suspicion of wrongdoing. It is not, and should not be, difficult for a customs officer to prove that a reasonable suspicion of wrongdoing existed prior to a search. Officers are trained to identify suspicious behavior and packages, as their suspicions are the first line of defense. Officers must be given latitude to rely on their suspicions to secure the U.S. border.

Some common "routine" border searches include "pat-downs, pocket-dumps, and even searches that require moving or adjusting clothing without disrobing, and also may include scanning, opening, and rifling through the contents of bags or other closed containers."[5] The Supreme Court has never directly articulated criteria to differentiate between "routine" and "nonroutine" border searches.[6] Rather, governing principles have been laid out in broad strokes, which can be summarized into a "reasonableness" test. In order for a "routine" border search to elevate to that of a "nonroutine" search, aggravating circumstances accompanied by a higher-than-normal level of intrusiveness must be present. The Supreme Court has held that "a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out."[7]

To illustrate this point, consider *United States v. Montoya de Hernandez*.[8] In this case, the respondent was suspected of smuggling narcotics in her alimentary cavity. She was initially detained and subject to a pat-down and strip search. During the search, it was discovered that her abdomen area felt "firm" and that she was wearing a special kind of undergarment generally associated with smuggling. The respondent was informed that she was a suspected smuggler and given the option to return to Colombia on the next available flight, agree to an X-ray, or remain in detention until she produced a monitored bowel movement. She was detained for almost sixteen hours before customs agents sought a court order authorizing a rectal examination. The exam revealed eighty-eight balloons containing nearly 530 grams of cocaine. The Court noted that the respondent's detention was long, uncomfortable, and humiliating, but neither its length nor discomfort made the detention unreasonable under the Fourth Amendment.[9] The search was reasonable, but the Court did, however, draw an important line. The circumstances and nature of respondent's detention and eventual search were not "routine." Nevertheless, officers were justified in acting the way they did because reasonable suspicion existed that the respondent was a drug smuggler.

More recently, two individuals were subject to airport searches by the federal government in a pair of widely publicized incidents. In January 2018, George Nader, a Middle East specialist with ties to President Trump, was stopped by the FBI at Dulles International Airport after returning to the United Stated from an overseas trip. Nader learned that Special Counsel Robert Mueller was interested in speaking to him regarding his involvement with key meetings between the United Arab Emirates and President Trump's associates. The FBI obtained a search warrant and imaged Nader's electronic devices. Nader was subsequently served with a grand jury subpoena. In March 2018, Ted Malloch, a political consultant connected to President Trump's election campaign, was detained by TSA and FBI agents and served with a subpoena at Boston's Logan Airport upon his return to the United States from London. Malloch's cell phone was confiscated, and he was advised that it would be analyzed for a full assessment.

Searching Electronic Devices: The Obama Administration Versus the Trump Administration

2009 Guidance/Operating Procedures

The same distinction between "routine" and "nonroutine" searches applies to data stored on electronic devices. "Nonroutine" searches still require at least a reasonable suspicion of wrongdoing. Under the Obama administration, CBP and ICE were permitted to conduct a quick, cursory ("routine") search of a traveler's electronic devices without a warrant or any suspicion of wrongdoing.[10] This could go so far as reading text messages and emails and viewing social media accounts. However, the courts have held that when sophisticated software is used to forensically analyze the information stored on an electronic device, such a search then becomes "nonroutine" and requires a reasonable suspicion of wrongdoing.[11]

Along with the authority to search a traveler's electronic devices, CBP and ICE are also empowered to detain, copy, and even share the information located on the device.[12] In most cases, if government officials keep an individual's electronic device, and that individual leaves the port of entry without it, the device is considered detained.[13] A traveler's electronic device may be detained without a warrant and without any individualized suspicion of wrongdoing. If a traveler's device is detained, there are two possible outcomes. The first is that CBP determines there is no evidence of criminal activity on the device, and it is returned to the individual in its original condition.[14] In addition, any copies of the information from the device that were made by CBP or ICE would then be destroyed.[15] The second possible outcome is that CBP determines that information found on the device merits referral to ICE. Now, here is where it gets interesting. According to previous CBP/ICE directives, when an electronic device is detained, CBP or ICE is permitted to seek technical assistance, including translation or decryption, from another person or entity, without a reasonable articulable suspicion that the data on the electronic device is evidence of a crime.[16] However, if ICE determined that it needs to bring in an outside entity to assist in analyzing the subject matter found on the device, a reasonable suspicion of wrongdoing was required.[17] In reality, this means that ICE could detain a traveler's phone for no reason at all and then bring in a third party to bypass the phone's password, decrypt its data, and search its contents.

2018 CBP Directive

On January 4, 2018, CBP released a new directive[18] to provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information found on electronic devices. The new directive supersedes the August 2009 policy directive that governed electronic devices searches throughout most of President Obama's time in office, as well as the majority of President Trump's first year.

Under the new directive, federal agents are still legally permitted to conduct a "basic" search of a traveler's electronic devices without a warrant and without an individualized suspicion of wrongdoing. CBP has defined a "basic search" as "[a]ny border search of an electronic device that is not an advanced search."[19] A basic search may consist of examining, reviewing, and analyzing information residing on a traveler's electronic device. An "advanced" search is "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."[20] To conduct an advanced search, officers must have a reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern. Many factors may create reasonable suspicion or constitute a national security concern; examples include "the existence of a relevant national security–related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list."[21]

Anyone crossing the border is obligated to unlock password-protected devices and decrypt data at the request of the investigating officer.

According to the directive, travelers are required to present their electronic devices in a condition that allows inspection of the device and its contents. This means anyone crossing the border is obligated to unlock password-protected devices and decrypt data at the request of the investigating officer. Failure to do so will likely result in the device being detained, allowing the officer to seek technical assistance in unlocking the phone, and/or decrypting data so that a search can take place. No level of suspicion is required for officers to seek technical assistance to gain access to protected devices.

One of the most important aspects of this directive is the prohibition on searching information that is stored remotely on cloud services. To avoid retrieving or accessing remotely stored information, officers have been instructed to either request that the traveler disable network connectivity or disconnect the device themselves when warranted by national security, law enforcement, officer safety, or other operational considerations.[22]

Searching "Privileged" Information

Additionally, when an officer encounters information he or she identifies as, or is asserted to be, protected by the attorney-client privilege or attorney work-product doctrine, the CBP directive under the Trump administration establishes strict procedures in continuing the search. First, the officer needs to seek clarification, preferably in writing, from the individual asserting the privilege as to specific information on the device that is privileged, such as specific files, names, email addresses, and phone numbers. Then, before any privileged information can be searched, the officer must next segregate any privileged information from other nonprivileged information. That will be done in coordination with the CBP Assistant Chief Counsel's office, which will also coordinate with the U.S. Attorney's Office as needed. As with any other electronic searches, at the completion of the CBP review, any copies of privileged information will be destroyed unless a national security threat is detected. In practice, CBP still has the authority to search and share information protected by the attorney-client privileged and the attorney work-product doctrine; it just must do so with the consent and advice of the appropriate government legal team.

The search of electronic devices at the border is a new frontier of the border search exception. As devices begin to hold more and more data, both CBP and civil rights groups are attempting to establish norms of what does and does not

fall within the exception. As is the case with any border search, the government and interested parties must continue to weigh the rights of the individual against national security interests.

Legal Challenges

Nonprofit groups, such as the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU), are seeking to challenge the current standards for searching a traveler's electronic devices at the border.[23] These groups argue four things:

(1) digital devices are both quantitatively and qualitatively different from physical containers, which the border search exception has traditionally applied to;

(2) the border search exception is narrow;

(3) the distinction between "routine" and "nonroutine" searches is constitutionally unworkable; and

(4) a warrant based on probable cause should be required to search digital data at the border.[24]

While electronic devices are qualitatively and quantitatively different from physical containers, this alone does not justify ignoring years of case law on the border search exception. It is true that our electronic devices house increasingly vast amounts of information, including emails, text messages, contact lists, medical

There is a lack of case law specifically differentiating between storage on an electronic device and storage in a suitcase.

records, business information, and social media accounts, among other things. As storage capacity continues to expand, there is a lack of case law specifically differentiating between storage on an electronic device and storage in a suitcase.[25]

This distinction, however, does not matter in the context of a border search analysis. Both the federal agencies conducting the search and the courts reviewing it have determined that a laptop, cell phone, or any other electronic device is subject to the same search as a traveler's "luggage" and "cargo."[26] As an example, if Mr. and Mrs. Smith are traveling across the border with a U-Haul carrying everything they own, would it be unreasonable to search the truck simply based on the quality or quantity of stuff that it contains? Absolutely not. The contents of the truck would be subject to the same search as every other vehicle crossing the border.

The sheer quality and quantity of cargo one carries does not impact the standard required to conduct a "routine" border search. Here's another way to think about it: Is a CBP officer going to spend weeks sorting through all the cargo Mr. and Mrs. Smith have packed into the U-Haul? In most cases, probably not. The officer is going to conduct a quick, cursory search of the contents to discover obvious violations. This applies to electronic devices as well. When CBP searches a traveler's phone, the search is limited to a manual search that must be reasonable in its application.

While the border search exception to the Fourth Amendment is narrow, a probable cause requirement would be an unprecedented and unnecessary limitation on the authority of CBP to conduct searches necessary to protect the U.S. border. In arguing for a probable cause standard, both the EFF and the ACLU rely heavily on the Supreme Court's ruling in *Riley v. California*.[27] There, the Court determined that police are required to obtain a probable cause warrant to search the cell phone of an individual under arrest, finding that the incident-to-arrest search exception does not apply to cell phones.[28] The Court in *Riley* acknowledged the privacy interests at stake in the digital data stored on a cell phone and concluded that "because of the immense quantity and scope of the information modern phones contain,"[29] the government's interest did not outweigh a reduced expectation of privacy with regard to cell phones.

An argument against the border search exception is easily made following the line of reasoning in *Riley*, but reliance on that Court's decision is misguided for one basic reason: the rationale behind the incident-to-arrest exception is fundamentally different from that of the border search exception. The incident-to-arrest exception allows an officer to reasonably search a suspect incident to arrest for officer safety and to preserve evidence the individual may be carrying

and able to conceal or destroy.[30] Allowing an officer to search a suspect's cell phone is not necessary for officer safety or evidence preservation, because an officer could easily protect himself and preserve evidence by simply taking the phone, shutting it off, and placing it into an evidence bag away from the suspect. Searching through the troves of digital data is not necessary to accomplish the end goal of the incident-to-arrest exception.

The reasonable suspicion standard works and should continue to be the standard required for the border search exception.

However, the border search exception operates for deterring unwanted persons and effects from entering the United States and allowing officers to search of a traveler's digital data directly serves that purpose. Doing so could reveal links to terrorist organizations, contraband, and general information that may be critical to an individual's admissibility. Requiring probable cause to allow for search of electronic devices would severely limit CBP's ability to determine potential national security risks.

Additionally, the reasonable suspicion standard is a workable standard for balancing individual privacy rights against national security concerns. While requiring reasonable suspicion leaves officers with considerable freedom to search suspicious persons and respond to unexpected factual developments, it also requires more than the typical suspicion of anyone crossing the U.S. border. Attempts to establish higher levels of scrutiny in the past have rightfully failed in the past. Take, for example, the previously mentioned case of *United States v. Montoya de Hernandez*, where the Supreme Court overruled a court of appeals decision establishing an intermediate standard between reasonable suspicion and probable cause. The Court stated that the reasonable suspicion standard "has been applied in a number of contexts and effects a needed balance between private and public interests when law enforcement officials must make a limited intrusion on less than probable cause."[31]

As electronic device storage capacity continues to expand, refinement of the border search exception will also continue. We must always keep in mind the incredibly important job of CBP: securing our nation's borders. The reasonable suspicion standard works and should continue to be the standard required for the border search exception. Additionally, CBP's distinction between device storage and cloud storage strikes the proper balance between the government's interest in policing the border and the individual privacy rights of an international traveler. The distinction made between "routine" and "nonroutine" border searches operates to safeguard the individual from unreasonable searches and provides officers with enough leeway to carry out their duties in preventing unwanted persons and effects from entering the country.

Rosanna Berardi is the founder and Managing Partner of Berardi Immigration Law, a business immigration law firm. She has a unique combination of government, university, and corporate experience that provides her with a broad perspective of the immigration landscape. This article is based on her PLI One-Hour Briefing "Right to Privacy at the Border Under the Trump Administration."

NOTES

1. U.S. Const. amend. IV.
2. United States v. Ramsey, 431 U.S. 606, 616 (1977).
3. Carroll v. United States, 267 U.S. 132, 154 (1925).
4. *Ramsey*, 431 U.S. at 616.
5. United States v. Saboonchi, 990 F. Supp. 2d 536, 549 (2014).
6. *Id.*
7. *Ramsey*, 431 U.S. at 618.
8. United States v. Montoya de Hernandez, 473 U.S. 531 (1985).
9. *Id.* at 544.
10. U.S. Customs & Border Prot., CBP Directive No. 3340-049, § 5.1 (Aug. 20, 2009), www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf; U.S. Immigration & Customs Enforcement, Directive No. 7-6.1, § 6.1 (Aug. 18, 2009), www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.
11. United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).
12. CBP Directive No. 3340-049, *supra* note 10, §§ 5.3.1, 5.4.1.
13. *Id.* § 5.3.1.1.
14. U.S. Dep't Homeland Sec., Privacy Impact Assessment for the Border Searches of Electronic Devices, at 7 (Aug. 25, 2009), www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.
15. CBP Directive No. 3340-049, *supra* note 10, § 5.3.1.2; ICE Directive No. 7-6.1, *supra* note 10, § 8.5(1)(e).
16. *See* 19 U.S.C. § 507; CBP Directive No. 3340-049, *supra* note 10, §§ 5.3.2.3–5.3.2.6.
17. ICE Directive No. 7-6.1, *supra* note 10, § 8.4 (Aug. 20, 2009).
18. U.S. Customs & Border Prot., CBP Directive No. 3340-049A (Jan. 4, 2018), www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf (superseding CBP Directive No. 3340-049, *supra* note 10).
19. *Id.* § 5.1.3.
20. *Id.* § 5.1.4.
21. *Id.*
22. *Id.* § 5.1.2.
23. *See* Complaint, Alasaad v. Duke, No. 1:17-cv-11730 (D. Mass. Sept. 13, 2017), www.eff.org/document/alasaad-v-duke-complaint.
24. Brief of Amicus Curiae Electronic Frontier Foundation in Support of Appellant, United States v. Saboonchi, No. 15-4111 (4th Cir. 2015), www.eff.org/document/eff-saboonchi-amicus-brief.
25. *See* United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013).
26. *See* United States v. Ickes, 393 F.3d 501, 504 (4th Cir. 2005).
27. Riley v. California, 134 S. Ct. 2473 (2014).

28. *Id*. at 2494.
29. United States v. Saboonchi, 48 F. Supp. 3d 815, 817 (2014).
30. Chimel v. California, 395 U.S. 752 (1969).
31. *Montoya de Hernandez*, 473 U.S. at 542.