



# Do Warrantless Searches of Electronic Devices at the Border Violate the Fourth Amendment?

December 20, 2019

The Fourth Amendment [commands that searches and seizures be reasonable](#), and generally requires the government to secure a [warrant based on probable cause](#) before arresting or searching an individual. But the Supreme Court has [long recognized](#) that the government may conduct routine inspections and searches of individuals entering at the U.S. border without a warrant or any individualized suspicion of criminal activity. In recent decades, some federal courts [have applied](#) the “border search exception” to allow [relatively limited, manual searches](#) at the border of electronic devices such as computers and cell phones. Courts, however, have disagreed over whether [more intrusive, forensic examinations](#) of such devices require heightened suspicion of criminal activity. Recently in *Alasaad v. Nielsen*, a federal district court ruled that any “non-cursory” border search of an electronic device—whether conducted manually or forensically—requires reasonable suspicion that the device contains contraband. The court’s decision could restrict the government’s ability to conduct border searches of electronic devices, which the government [contends](#) is essential to prevent crimes and protect border security. This Legal Sidebar examines the application of the Fourth Amendment’s border search exception to searches of electronic devices and the district court’s decision in *Alasaad* limiting the government’s border search authority.

## The Fourth Amendment and the Border Search Exception

Under the Fourth Amendment the government generally must [obtain a warrant](#) based on probable cause before arresting or searching an individual. To show probable cause, the government must present facts evidencing a [reasonable belief](#) that an individual has likely committed a criminal offense. The Fourth Amendment may also limit certain governmental searches and seizures conducted in [non-criminal, civil proceedings](#) (e.g., building inspections, involuntary civil commitment). The Supreme Court, however, has held that the government may engage in a [warrantless arrest or search](#) in certain circumstances. For example, in the criminal context, the government may bypass the warrant requirement if an arrest [occurs in public and is based on probable cause](#), or if a search is [incident to a lawful arrest](#). Additionally, warrantless searches and seizures of [limited duration and intrusiveness](#), such as a “stop and frisk,” may be permitted if there is reasonable suspicion of criminal activity. This standard, [lower](#) than the probable cause threshold for an arrest, requires specific, articulable facts—rather than a mere hunch—that reasonably warrant suspicion of criminal activity. And in the civil immigration context, [several courts](#)

Congressional Research Service

<https://crsreports.congress.gov>

LSB10387

have held or suggested that the Fourth Amendment requires an immigration-related detention to be predicated on at least reasonable suspicion that an individual may be subject to removal.

Under the border search exception, the government may engage in routine inspections and searches of individuals at the U.S. border without probable cause *or* reasonable suspicion of criminal activity. Citing the federal government's power to regulate the flow of people and goods across the border, the Supreme Court has reasoned that "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior" of the United States, and there is less expectation of privacy at the border. The Court has applied this exception not only to the physical border itself, but also to searches at the border's "functional equivalent," such as an international airport in the interior of the United States or a fixed roadside checkpoint near the U.S. border.

That said, a border search that extends beyond a routine search and inspection may require at least reasonable suspicion of criminal activity. The Supreme Court has not precisely defined the scope of a routine border search, but the Court has listed "strip, body cavity, or involuntary x-ray searches" as falling outside that category. The Court has also suggested that non-routine border searches may include "highly intrusive searches" that breach personal dignity and privacy interests, or cause the destruction of property. Thus, the Court has held that the prolonged detention of a traveler pending a pregnancy test and rectal examination required reasonable suspicion that she was an alimentary canal drug smuggler. On the other hand, the search of an automobile fuel tank and the opening of international mail have been considered routine border searches. Lower federal courts have also addressed the scope of a routine border search, holding that it may include the suspicionless search of closed containers, papers, luggage, purses, wallets, pockets, and photographs.

## Judicial Application of the Border Search Exception to Searches of Electronic Devices

The Supreme Court has not addressed whether the routine border search exception extends to searches of electronic devices such as cell phones—items that may contain more personal and sensitive information than what would typically be found inside a traveler's briefcase or automobile. But in 2014 the Court in *Riley v. California* considered the constitutionality of warrantless electronic device searches in the interior of the United States. The Court held that the police generally could not conduct a warrantless search of a cell phone seized during an arrest, even though the warrant requirement usually does not apply to searches incident to a lawful arrest. Noting that this exception ordinarily applies to brief physical searches of property within the immediate control of the arrestee to prevent potential harm to the police officers and the destruction of evidence, the Court determined that "[t]here are no comparable risks when the search is of digital data." The Court also concluded that searching cell phone data raises greater privacy concerns than searching physical items typically found on a person (e.g., a wallet). The Court observed that cell phones, unlike most other physical items, contain "immense storage capacity" and carry a broader range of private information, including photographs, videos, contacts, text messages, financial records, and Internet browsing history. The Court thus held that the police generally must secure a warrant before searching the contents of a cell phone seized pursuant to an arrest. But the Court noted that "other case-specific exceptions may still justify a warrantless search of a particular phone."

Lower courts have considered whether the routine border search exception authorizes warrantless searches of cell phones and other electronic devices at the border. For instance, the U.S. Courts of Appeals for the Fourth and Ninth Circuits have held that manually inspecting the contents of a computer or cell phone at the border is permissible given the government's broad authority at the border, and that such searches are no less routine than scanning the contents of a traveler's luggage. But lower courts have disagreed over whether more intrusive searches of electronic devices require particularized suspicion of criminal activity. The Fourth and Ninth Circuits have both held that the forensic examination of a device

(e.g., using software to copy a computer's hard drive and analyze its contents entirely, or recording information from a cell phone for further processing) exceeds the scope of a routine border search because of its comprehensive nature and the enhanced risk of exposing private information. In doing so, both courts relied on the Supreme Court's reasoning in *Riley* that cell phone searches implicate greater privacy concerns than searches of most other physical items. Thus, the Fourth and Ninth Circuits have held that forensic searches of electronic devices require reasonable suspicion of a crime. Conversely, the [Eleventh Circuit](#) has held that the Fourth Amendment requires no suspicion of criminal activity for intrusive border searches of electronic devices or any other type of personal property (as opposed to intrusive searches of a person's body), and that *Riley* does not apply to searches at the border, where there are diminished privacy expectations.

In sum, while lower courts have applied the routine border search exception to cover manual searches of electronic devices at the border, courts have disagreed on whether more intrusive, forensic searches of such devices should be restricted.

## The Department of Homeland Security's Current Policies on Border Searches of Electronic Devices

The Department of Homeland Security's (DHS) [Customs and Border Protection](#) (CBP), the agency primarily responsible for enforcing customs and immigration laws along the international borders and at U.S. ports of entry, typically conducts any initial search or inspection of an electronic device. The agency [defines](#) an electronic device to include "any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players." DHS's [Immigration and Customs Enforcement](#) (ICE), the agency primarily responsible for immigration enforcement in the interior of the United States, as well as the investigation of cross-border criminal activity, may also play a role. For example, when CBP seizes or detains an electronic device, it may [turn over the device](#) to ICE for analysis and investigation.

Previously, both [CBP](#) and [ICE](#) authorized electronic device searches at the border "with or without individualized suspicion" of criminal activity. But more recently, the agencies issued [superseding policies](#) that distinguish between a "basic search" and an "advanced search" of an electronic device. A [basic search](#) is described simply as any electronic device search that is "not an advanced search," and involves a manual examination of the electronic device and its contents. The basic search may be conducted "with or without suspicion" of criminal activity. An [advanced search](#) occurs when a CBP or ICE official "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" (i.e., a forensic search). Both CBP and ICE policies [provide that](#) an advanced search may occur only upon reasonable suspicion of criminal activity (CBP also authorizes an advanced search if there is a "national security concern"). In addition, CBP's policy [authorizes](#) officers to "detain" an electronic device (or copies of information contained within it) "for a brief, reasonable period of time to perform a more thorough border search," generally not exceeding a period of 5 days. And CBP officers may [seize and retain](#) an electronic device (or copies of information from the device) if there is probable cause that the device contains evidence of a crime.

## The Federal District Court's Decision in *Alasaad v. Nielsen*

In *Alasaad v. Nielsen*, ten U.S. citizens and one [lawful permanent resident](#) (plaintiffs) had their cell phones or other electronic devices [searched](#) by CBP or ICE officials upon their return to the United States following trips abroad. Plaintiffs [claimed](#) that the officials had threatened to confiscate their devices if they refused to provide their passwords to unlock them, or that they otherwise felt coerced to provide access to their devices. Plaintiffs alleged that, upon unlocking their devices, the officers [viewed private information](#), such as photographs, work product, and [attorney-client communications](#). In some instances,

the officers confiscated the devices or retained information collected from them. The plaintiffs filed a [lawsuit](#) in the U.S. District Court for the District of Massachusetts, arguing that the warrantless searches of their electronic devices violated the Fourth Amendment. They further claimed that CBP and ICE violated the First Amendment because the searches disclosed “expressive content and associational information.” In a [motion for summary judgment](#), the plaintiffs [asked](#) the court to declare the agencies’ practices unconstitutional and to issue an injunction prohibiting them from searching electronic devices without a warrant supported by probable cause. In response, the government [argued](#) that the border search exception permits the government to search electronic devices without a warrant or probable cause.

The federal district court [granted](#), in part, the plaintiffs’ motion. The court first [noted](#) that the border search exception grants the government broad authority to conduct warrantless searches and seizures at the U.S. border without a particularized suspicion of criminal activity. But the court [recognized](#) that this exception applies to routine border searches and not to highly intrusive searches. The court [determined](#) that the Supreme Court’s conclusion in *Riley v. California* that cell phone searches implicate greater privacy concerns than other types of searches incident to an arrest “holds the same force when applied to border searches.” The court [declared](#) that “[t]he potential level of intrusion from a search of a person’s electronic devices simply has no easy comparison to non-digital searches.”

Informed by the Supreme Court’s reasoning in *Riley*, the district court [held](#) that the electronic device searches authorized by CBP’s and ICE’s policies go beyond the scope of a routine border search. The court [explained](#) that, although CBP and ICE authorize either basic or advanced searches of electronic devices, both types of searches “implicate the same privacy concerns” at stake in *Riley*. The court [reasoned](#) that, in a basic search, CBP or ICE officers can manually scan and search the contents of the device and access “a wealth of personal information.” And for advanced searches, the court noted that they can reveal an even “[broader range](#)” of information, including deleted or encrypted data, and that such searches enable the copying of information from the device.

The court [distinguished](#) the potentially intrusive searches permitted under a basic or advanced search from a general “cursory search” of an electronic device, which “would fall within the border search exception and not require a heightened showing of cause.” The court [described](#) a cursory search as “a brief look reserved to determining whether a device is owned by the person carrying it across the border, confirming that it is operational and that it contains data.” Because basic and advanced searches, by contrast, involve a greater “intrusion into personal information,” the court [ruled](#) that they [require reasonable suspicion](#) that an electronic device contains contraband (i.e., goods that are illegally imported or exported). The court declined to impose the heightened requirement that the government obtain a warrant supported by probable cause to conduct the search, as the plaintiffs had requested, [reasoning](#) that “the governmental interests are different at the border” than in the interior of the United States.

The court also [considered](#) the plaintiffs’ contention that the warrantless search of “expressive materials” within their electronic devices violated the First Amendment. Plaintiffs [had alleged](#) that their First Amendment rights were implicated because their devices contained “highly sensitive information concerning their personal, privileged, confidential, and anonymous communications and associations.” The court [concluded](#) that the reasonable suspicion standard adopted for non-cursory border searches of electronic devices could also be applied to searches that raise First Amendment concerns. Thus, the court [determined](#) that it was unnecessary to issue any further ruling with respect to the First Amendment claim.

The court thus [held](#) that the non-cursory searches of the plaintiffs’ electronic devices without reasonable suspicion violated the Fourth Amendment. Subsequently, in a separate order, the court issued an injunction barring CBP and ICE from conducting a border search or seizure of any electronic device owned by the plaintiffs unless the agencies have reasonable suspicion that the device contains contraband. The court further ruled that, in the event CBP and ICE have the requisite reasonable suspicion, they are barred from detaining the electronic device “longer than a reasonable period that allows for an investigatory search for that contraband.”

## Implications of *Alasaad* and Other Considerations

Under the border search exception, the government may conduct routine searches at the border or its functional equivalent without a warrant or any particularized suspicion of criminal activity. Previously, courts have applied this exception to relatively limited, manual searches of electronic devices. But some courts have held that more intrusive, forensic searches require at least reasonable suspicion of criminal activity. In reaching this conclusion, some courts have relied on the Supreme Court's decision in *Riley v. California*, reasoning that the significant privacy interests implicated by warrantless cell phones searches incident to an arrest apply equally to forensic searches of electronic devices at the border.

Citing *Riley*, the federal district court in *Alasaad v. Nielsen* appears to go a little further, requiring reasonable suspicion not only for "advanced" forensic searches of electronic devices, but also for "basic" *manual* searches that are not "cursory"—that is, confined to confirming that a device is operational and stored with data. Put another way, under *Alasaad*, any *non-cursory* border search of an electronic device—whether conducted manually or forensically—must be supported by at least reasonable suspicion to withstand Fourth Amendment scrutiny. The court's ruling could considerably limit DHS's ability to conduct border searches of electronic devices. Currently, CBP and ICE [allow](#) basic manual searches of electronic devices "with or without individualized suspicion," and only require heightened suspicion for advanced, forensic searches. Under *Alasaad*, manual border searches of electronic devices may, absent reasonable suspicion, be limited to turning on the device and verifying that it has data. Any further action—including searching the contents of the device—would require at least reasonable suspicion of a crime.

*Alasaad* raises questions about the interplay between the Supreme Court's decision in *Riley* and the border search doctrine. On one hand, the *Riley* decision [recognizes](#) that searches of cell phones implicate privacy concerns "far beyond" those implicated by the search of other physical items like wallets or purses. On the other hand, the border search doctrine [instructs](#) that "the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border," and that "the expectation of privacy is less at the border than it is in the interior." But does that balance of interests change when a border search extends to cell phones and other electronic devices? As the Supreme Court noted in *Riley*, cell phones are basically "minicomputers" that can store a vast amount of "sensitive personal information" not typically found inside a wallet or even a home. Arguably, these privacy interests are no less significant at the border.

Further, if the privacy concerns implicated by cell phone searches in *Riley* extend to border searches, at what point should there be restrictions on such searches? As discussed above, some courts have applied *Riley* to restrict [only forensic searches](#) of electronic devices, while the *Alasaad* court would restrict any *non-cursory* search. Courts have also [disagreed](#) about whether the border searches should be limited in scope to searching for digital contraband within the electronic device itself (e.g., child pornography), or whether they may extend to searching for any evidence of a crime (e.g., examining device to determine whether there is evidence that a person was attempting to export firearms). The Eleventh Circuit, meanwhile, has [held](#) that *Riley* does not apply at all to border searches, and that the Supreme Court has never required heightened suspicion for border searches of *property*—no matter how intrusive. At some point the Supreme Court may decide to resolve these questions and determine the extent to which the border search exception applies to searches of electronic devices.

## Recent Legislative Activity

Given judicial disagreement over the extent to which the government may conduct warrantless searches of electronic devices at the border, Congress may choose to clarify that authority. In the 116th Congress, legislation has been introduced that generally restricts the government's border search power. For example, one bill ([S.2694](#)) would allow a manual electronic device search (which is defined to include



any manual examination of the device) only upon reasonable suspicion that (1) the individual transporting the device is carrying contraband or engaged in certain other specified activity, and (2) the device contains evidence relevant to the contraband or specified activity. The bill would allow the seizure of an electronic device only upon probable cause that (1) the individual is carrying contraband or engaged in certain other specified activity, or has violated any law punishable by more than one-year imprisonment, and (2) the device contains evidence related to the contraband, specified unlawful activity, or criminal violation. The bill would permit a forensic search (which is defined to include a search that uses software or external equipment, involves copying of data, is conducted for more than 4 hours, or is conducted manually with the entry of a password) only pursuant to a warrant. The bill would also set forth certain procedures for electronic device searches (e.g., obtaining supervisory approval), and require a warrant or court order no later than 48 hours after the seizure of a device.

A separate bill, the Protecting Data at the Border Act ([S.1606](#), [H.R.2925](#)), would prohibit the government from accessing the digital contents of an electronic device belonging to a “United States person” (defined to include a U.S. citizen and a lawful permanent resident) without a warrant supported by probable cause; and denying a United States person’s entry into or exit from the United States based on his or her refusal to provide access to the device. If a United States person consents to providing access to his or her electronic device, the bill would require the government to obtain the consent in writing (with written advisals indicating that access to the device cannot be compelled without a valid warrant) before accessing the device. The bill would also prohibit the government from delaying a United States person’s entry into or exit from the United States for more than 4 hours pending a determination as to whether that person will consent to providing access to the device. The bill further provides for certain “emergency exceptions” to the warrant requirement (e.g., if a CBP officer reasonably determines that an emergency situation exists that involves potential death or serious physical injury to any person, and that the situation requires immediate access to the contents of the electronic device).

## Author Information

Hillel R. Smith  
Legislative Attorney

---

## Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS’s institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.

---

