Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

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

Updated March 17, 2021

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. Mayorkas*, the U.S. Court of Appeals for the First Circuit overturned a federal district court's ruling that any "non-cursory" border search of an electronic device—whether conducted manually or forensically—requires reasonable suspicion that the device contains contraband. This Legal Sidebar examines the application of the Fourth Amendment's border search exception to searches of electronic devices and the *Alasaad* litigation concerning the reach of the government's border search authority. A more extensive analysis of the Fourth Amendment's application at the border is available in a CRS Report.

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 noncriminal, 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 nonroutine 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's) 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 five 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.

Litigation in *Alasaad v. Mayorkas*

In *Alasaad v. Mayorkas*, 10 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. 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."

The federal district court granted, in part, the plaintiffs' motion for summary judgment. Informed by *Riley's* conclusion that cell phone searches are more invasive than searches of other physical items, the court held that the electronic device searches authorized by CBP's and ICE's policies go beyond routine border searches. The court reasoned that, in a basic search, CBP or ICE officers can manually scan the contents of the device and access "a wealth of personal information." And for advanced searches, the court noted they can reveal an even "broader range" of information, including deleted or encrypted data. The court distinguished these types of searches from a limited "cursory search," which "would fall within the border search exception." The court thus ruled that basic and advanced searches require reasonable suspicion that an electronic device contains contraband. The court declined to require a warrant supported by probable cause to conduct the search, reasoning that "the governmental interests are different at the border" than in the interior of the United States. The court also ruled that, in the event CBP and ICE have reasonable suspicion, they may not detain the electronic device "longer than a reasonable period that allows for an investigatory search for that contraband." As for plaintiffs' First Amendment claim, the court concluded that the reasonable suspicion standard could also be applied to electronic device 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.

Both the government and plaintiffs appealed the district court's decision. On February 9, 2021, the First Circuit partially reversed and vacated the district court's decision, concluding that the challenged border search policies "are within permissible constitutional grounds." First, the appellate court rejected plaintiffs' contention that electronic device border searches require a warrant in light of the Supreme Court's decision in *Riley*. The court explained that *Riley* does not mandate a warrant requirement for all electronic device searches, and that the Supreme Court's decision does not apply to border searches, "which are entirely separate from the search incident to arrest searches discussed in *Riley*." According to the First Circuit, "a warrant requirement—and the delays it would incur—would hamstring the agencies' efforts to prevent border-related crime and protect this country from national security threats."

The First Circuit also rejected plaintiffs' argument, in the alternative, that all electronic device searches under the CBP and ICE policies, including basic searches, require reasonable suspicion. Recognizing that electronic device searches implicate greater privacy concerns than searches of other physical items, the court reasoned that these concerns "are nevertheless tempered by the fact that the searches are taking place at the border," where there is a heightened interest in preventing the entry of unwanted persons and goods. The court also observed that a basic electronic device search does not involve an intrusive search of a person, and is limited to accessing information on the device itself. The court thus held that a basic electronic device search at the border is a routine search requiring no reasonable suspicion (The First Circuit left undisturbed the district court's ruling that *advanced* searches require reasonable suspicion; but, as noted, both CBP and ICE policies currently require reasonable suspicion for such searches.)

With regard to the scope of an electronic device border search, the First Circuit disagreed with the plaintiffs' contention that the search should be limited to searching for contraband only. The court reasoned that, given the government's paramount interest in preventing the entry of harmful persons and effects at the border, the border search exception covers not only searching for contraband itself, but also *evidence* of contraband or border-related crime. The court thus held that "advanced border searches of electronic devices may be used to search for contraband, evidence of contraband, or for evidence of activity in violation of the laws enforced or administered by CBP or ICE."

Finally, the First Circuit rejected plaintiffs' assertion that the government's search of their electronic devices and exposure of expressive information violates the First Amendment. The court determined that

the content-neutral search policies adopted by CBP and ICE "have a plainly legitimate sweep and serve the government's paramount interests in protecting the border." In the court's view, the presence of expressive material on electronic devices does not require a warrant or a heightened level of suspicion.

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. Mayorkas* appeared 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. The court's ruling could have considerably limited DHS's ability to conduct border searches of electronic devices. But as discussed above, the First Circuit has partially reversed the district court's decision, holding that basic, manual searches of electronic devices fall squarely within the border search exception as routine searches, and thus require no reasonable suspicion. Thus, the First Circuit's decision reinforces long-standing precedent holding that federal officers may conduct routine searches at the border without a warrant or any particularized suspicion of a crime.

Alasaad and other litigation concerning the government's ability to search electronic devices at the border raise 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, a person's privacy interests in such material is no less significant at the border.

But even 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 district court in *Alasaad* would have restricted 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, as the First Circuit has held when *Alasaad* came before it on appeal, the search may extend to looking for any evidence of a crime (e.g., examining a device to determine whether it contains evidence of ongoing border-related crimes, such as the illegal importation of 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. To date, no legislation directly addressing this issue has been introduced in the 117th Congress. But in the 116th Congress, legislation was introduced that would have generally restricted the government's border search power. For example, one bill (S. 2694) would have allowed a manual electronic device search (which was 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 have allowed 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 have permitted a forensic search (which was defined to include a search that uses software or external equipment, involves copying of data, is conducted for more than four hours, or is conducted manually with the entry of a password) only pursuant to a warrant. The bill would have also set forth certain procedures for electronic device searches (e.g., obtaining supervisory approval), and required 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 have prohibited 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 consented to providing access to his or her electronic device, the bill would have required 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 have prohibited the government from delaying a United States person's entry into or exit from the United States for more than four hours pending a determination as to whether that person would consent to providing access to the device. The bill further provided 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