# Court of Appeals affirms broad government authority to conduct warrantless searches of electronic devices at the border

White Collar Alert

16 February 2021
By: John M. Hillebrecht | Eric P. Christofferson | Paul B. Lewis

In a recent opinion, the United States Court of Appeals for the First Circuit affirmed the constitutionality of so-called “basic” or “routine” searches of electronic devices at the border – absent a warrant, probable cause or even reasonable suspicion. Given the volume and sensitivity of information increasingly stored on phones and other devices, the court’s opinion offers a reminder that personal privacy is at significant risk when traveling abroad or returning home.

**Background**

The appeal in *Alasaad v. Mayorkas*, Nos. 20-1077, 20-1081, 2021 U.S. App. LEXIS 3586 (1st Cir. Feb. 9, 2021), involved a civil suit in which ten US citizens and one lawful permanent resident sought declaratory and injunctive relief, alleging that officers from the US Customs and Border Protection Agency and the US Immigration and Customs Enforcement Agency (together, the Agencies) searched their respective electronic devices at the nation’s ports of entry without a warrant, probable cause or reasonable suspicion – pursuant to the Agencies’ own internal policies (the Policies).

Beginning in 2018, the Policies defined both “basic” and “advanced” searches of electronic devices. A so-called “advanced” search is any search of an electronic device conducted in order to review, copy or analyze its contents, which may involve the use of external equipment. It may also extend to deleted or encrypted files. To justify such a search, the Agency must have reasonable suspicion that the search will yield evidence of criminal activity.

By contrast, a so-called “basic” search is relatively limited in duration, must be conducted manually (ie, without the use of external equipment) and does not extend to deleted or encrypted files. As the District Court noted, the “basic” searches at issue lasted approximately 45 minutes and involved the viewing of emails and text messages. The Agency may conduct such a search without any suspicion of criminal activity. Notably, the Policies require for both “basic” and “advanced” searches that the device must be disconnected from the internet before the search can commence.

Each of the plaintiffs alleged that, at various ports of entry (mostly international airports), they had their laptops or smartphones temporarily seized, and their contents searched, by Agency personnel – without any warrant, probable cause or articulable degree of suspicion. In most cases, the individuals provided their passwords after what they understood to be orders to do so.

**First Circuit’s opinion**

After the lower court granted in part and denied in part the plaintiffs’ motion for summary judgment, the First Circuit considered the plaintiffs’ arguments – grounded in both the Fourth and the First Amendments – de novo. Specifically, the plaintiffs argued that (i) all electronic device searches at the border require a warrant, and that, in the alternative, (ii) all electronic device searches at the border require, at least, reasonable suspicion that the device contains contraband.

The plaintiffs primarily based their challenge on the US Supreme Court’s opinion in *Riley v. California*, 573 U.S. 373, 382 (2014), which held that a warrantless search incident to arrest cannot extend to the electronic contents of a cell phone. *Riley*, however, did not involve an arrest or search at the border.

For the reasons further detailed below, the First Circuit rejected all of the plaintiffs’ arguments.

> **Basic electronic device searches at the border require neither warrants nor reasonable suspicion**
>
> The court quickly dispatched the plaintiffs’ argument that either a warrant or probable cause is necessary to conduct any search. It began by placing the searches at issue squarely within the “border search” exception to the general warrant requirement. Previously endorsed by the US Supreme Court, this exception is grounded in the government’s inherent authority to protect its territorial integrity. In fact, the expectation of privacy at the border is markedly lower than the expectation of privacy in the nation’s interior.
>
> The court further explained that, given the volume of travelers passing through the nation’s borders, warrantless electronic device searches are essential. More specifically, it opined that the Executive Branch will only be able to adequately protect the border if it is not subject to the warrant requirement because the resulting delays would necessarily hamstring its efforts to protect the country from national security threats.
>
> In turning to the next level of justification – reasonable suspicion – the court analogized “basic” searches under the Policies to “routine” searches of other property at the border which the Supreme Court has previously held can be performed without any degree of suspicion. In the First Circuit, permissible “routine” property searches have been held to include, for example, the compelled removal of an outer layer of clothing. See *United States v. Braks*, 842 F.2d 509, 513 (1st Cir. 1988). By contrast, however, a search that is not “routine,” such as an “advanced” search under the Policies, must be justified by, at least, reasonable suspicion. Whether a search is “routine” or “non-routine” has traditionally been a fact-specific inquiry.
>
> The court distinguished prior opinions (like the Supreme Court’s decision in *Riley*) that have remarked upon the significant privacy interests necessarily affected by electronic device searches in non-border contexts, from such searches when they occur at the border. The court stated that, there, the government’s interest in preventing the entry of unwanted persons and effects is at its zenith. Accordingly, the First Circuit concluded that searches may include looking for evidence of crimes, thereby rejecting the plaintiffs’

request to simply limit them to contraband.

After explaining the limits of Fourth Amendment protection, the court noted that Congress and the Executive Branch are certainly free to grant individuals *greater* protection than that afforded by the Constitution.

**No express limit set as to duration of detention of devices searched**

The court declined to set a bright-line rule as to the appropriate duration of a device's seizure, remarking that the plaintiffs did not present any facts about the actual length of the detentions at issue. Instead, the court indicated that the relative reasonableness of the duration will be decided on a case-by-case basis.

Notably, however, the Policies require supervisory approval to extend a device detention beyond 5 days (under the Customs and Border Patrol Policy) and 30 days (under the Immigration and Customs Enforcement policy). Such approval is also necessary if the devices are to depart from the location of their initial detention. As to the scope of the initial search, the Policies state only that a "basic" search must be both brief and reasonable.

**The First Amendment does not provide any additional protection in this context**

The plaintiffs also asserted that these searches mandated the compelled disclosure of expressive information, thereby violating the First Amendment. After remarking that neither the First Circuit nor the US Supreme Court has identified an appropriate standard through which First Amendment intrusions at the border might be assessed, the court rejected this challenge as well. In doing so, the court focused on the fact that the Policies are content-neutral. It also reiterated the government's paramount interests in protecting the nation's border.

The plaintiffs' argument that a higher level of suspicion would be required to search expressive material was similarly rejected. Citing Ninth Circuit precedent, the court explained that drawing such a distinction for expressive material would be unworkable in practice and would potentially protect important terrorist communications.

The court expressly left open the question of whether the outcome of a First Amendment challenge to the Policies would be different if there were reason to believe that the agencies were specifically targeting journalists.

**Key takeaways**

The First Circuit's opinion underscores the risks that one takes when entering the country while in possession of sensitive material and information.

Significantly, the court expressly passed on deciding whether the disclosure of the plaintiffs' passwords – the circumstances surrounding which varied widely among the plaintiffs – was constitutional. Therefore, it is at least likely that using passwords will continue to provide some protection, at least from such "basic" searches in the absence of reasonable suspicion. Ultimately, if no level of suspicion that the contents of the phone might contain evidence exists, the Policies would preclude an "advanced" search. In this circumstance, it is quite difficult to envision a scenario in which the agents could access a phone's contents absent an individual's voluntarily providing their password.

Additionally, in non-border contexts, other jurisdictions have deemed it violative of the Fourth Amendment to *compel* individuals to provide their passwords without cause, and a petition for a writ of certiorari is currently pending before the Supreme Court concerning whether the Fifth Amendment protects an individual from being compelled to disclose a passcode. See Petition for Writ of Certiorari, *Andrews v. New Jersey*, (No. 20-937). However, given its highly permissive view of border searches, the First Circuit could theoretically distinguish such holdings in the future in that specific context.

As noted above, under the Agencies' Policies at issue in *Alasaad*, a "basic" search must be conducted manually, must be limited in time and scope, and must occur only at the location of the seizure. Therefore, it seems unlikely that Agencies could access an individual's locked data if the device's owner does not voluntarily unlock the device, or alternatively provide its password. And, under the Policies, if more complex methods of accessing the contents

of a device are to be employed, then an articulable degree of suspicion is likely required because that would probably entail an “advanced” search.

Of course, although perhaps easier said than done, travelers can protect themselves and their employers by taking certain precautions:

- *First*, travelers can avoid storing any particularly sensitive data on the actual device. Indeed, the Policies expressly limit all “basic” searches to information contained on the electronic device itself, and all searches require the device to be disconnected from the internet. Thus, storing particularly sensitive data on the “cloud,” as opposed to saving it within the device’s physical memory, could provide more protection.

- *Second*, heightened precautions may be prudent to the extent that an individual works for an entity that is under criminal investigation because particular employees may be under a “border watch,” resulting in them being singled out upon arrival at the border. In that scenario, it is imperative that employees not bring any hard copy files or any electronic devices containing company or privileged data into the United States. In some extreme circumstances, it can be appropriate for employees traveling to the United States to bring “clean” (ideally brand new) electronic devices for use during their trip. The devices should not contain any emails or other documents. Of course, it may be difficult to conduct business in the United States without access to any company documents. If necessary, an employee can consider loading the files needed to conduct meetings onto the “clean” device, but he or she should make every effort to minimize the historic data included.

- *Third*, if employees must bring company data into the United States, we recommend that they encrypt and password-protect each electronic device and that they store each set of files in separate password-protected folders. We also recommend that sensitive information be marked “Confidential.” In addition, if employees must bring legally privileged material into the United States, we recommend that they separately label those documents as well.

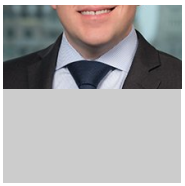
- *Fourth*, if an agent requests the password to an employee’s computer (or requests that the employee unlock the computer) with sensitive company documents on it, the employee should (if accurate and truthful): (a) tell the agent that the computer contains confidential and privileged information and request the agent check with the Customs Office of General Counsel before proceeding; and (b) state that the electronic device(s) may contain documents subject to the attorney-client privilege and request the opportunity to call his or her attorney or company counsel. If the agent persists after the employee refuses to provide the password or unlock the device, however, the agent may ultimately seize the device or take other steps.

In sum, while the court’s opinion in *Alasaad* authorizes expansive search authority at the border, some common-sense protective measures should offer travelers, employees and employers some comfort.

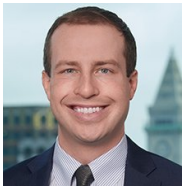
## AUTHORS


**John M. Hillebrecht**
Partner
New York | T: +1 212 335 4500
john.hillebrecht@dlapiper.com

**Eric P. Christofferson**
Partner
Boston | T: +1 617 406 6000



eric.christofferson@dlapiper.com



**Paul B. Lewis**
Associate
Boston | T: +1 617 406 6000
paul.lewis@dlapiper.com