ALERT MEMORANDUM

First Circuit Upholds Border Searches of Electronic Devices Without Probable Cause

February 25, 2021

In a decision with potentially far-reaching implications, *Alasaad v. Mayorkas*, Nos. 20-1077, 20-1081, 2021 WL 521570 (1st Cir. Feb. 9, 2021), the First Circuit recently rejected First and Fourth Amendment challenges to the U.S. government agency policies governing border searches of electronic devices. These policies permit so-called "basic" manual searches of electronic devices without any articulable suspicion, requiring reasonable suspicion only when officers perform "advanced" searches that use external equipment to review, copy, or analyze a device. The First Circuit held that even these "advanced" searches require neither probable cause nor a warrant, and it split with the Ninth Circuit in holding that searches need not be limited to searches for contraband, but may also be used to search for evidence of contraband or evidence of other illegal activity.

This decision implicates several takeaways for company executives entering and leaving the United States – citizens and non-citizens alike – particularly if they or their employers are under active investigation. In-house counsel in particular should consider the implications of the decision given obligations of lawyers to protect the confidentiality of attorney-client privileged information.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

David E. Brodsky
+ 1 212 225 2910
dbrodsky@cgsh.com

Lev L. Dassin
+ 1 212 225 2790
ldassin@cgsh.com

Victor L. Hou
+ 1 212 225 2609
vhou@cgsh.com

Rahul Mukhi
+ 1 212 225 2912
rmukhi@cgsh.com

Giovanni P. Prezioso
+ 1 202 974 1650
gprezioso@cgsh.com

Samuel Levander
+ 1 212 225 2951
slevander@cgsh.com

Background

Traditionally, courts have held that searches at the border "are reasonable simply by virtue of the fact that they occur at the border," where the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith."[1] "[T]he expectation of privacy is less at the border than it is in the interior," and officers at the border generally may, without any articulable suspicion, search through travelers' bags and other personal items.[2] The Supreme Court has historically taken a broad view of the border exception, holding that it extends to any "routine" searches, including opening a sealed letter,[3] and disassembling a car's gas tank.[4] It has, however, drawn the line at "non-routine" searches, such as certain particularly invasive body searches, which it has held require reasonable suspicion.[5]

More recently, there has been extensive litigation over the standard of suspicion required to search a traveler's electronic devices, such as cell phones and laptops. While these searches are less physically intrusive than those previously identified by the Supreme Court as "non-routine," there is a growing consensus that, with developments in technology, searches of electronic devices implicate fundamental privacy interests and may reveal "far *more* than the most exhaustive search of a house."[6]

CBP and ICE Guidelines for Searching Devices at the U.S. Border

In 2018, U.S. Customs & Border Protection ("CBP") announced new search guidelines for electronic devices at the border.[7] These guidelines differentiated between "basic" searches, which involve a manual examination of a device's contents, and "advanced" searches, which rely on external equipment to review, copy, or analyze a device's contents.[8] The guidelines are equally applicable to U.S. citizens and non-citizens.

Under the CBP guidelines, a basic search can be performed without any basis for suspicion whatsoever, while an advanced search requires reasonable suspicion of criminal activity or a national security concern.[9]

For either search, CBP officers may seek travelers' assistance in opening any password-protected device.[10] If a traveler does not provide such assistance, or if CBP is otherwise unable to complete an inspection because of password or encryption protection, the officer may temporarily detain or permanently seize the device.[11]

---

[1] *United States v. Flores-Montano*, 541 U.S. 149, 152, 154 (2004) (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)); *see Boyd v. United States*, 116 U.S. 616, 623 (1886) ("[I]t is clear that the members of that body did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the [Fourth Amendment].").

[2] *Ramsey*, 431 U.S. at 616; *see United States v. Irving*, 452 F.3d 110, 123-24 (2d Cir. 2006) ("[W]e have long ruled that searches of a person's luggage or personal belongings are routine searches.").

[3] *Ramsey*, 431 U.S. 606.

[4] *Flores-Montano*, 541 U.S. 149.

[5] *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985) ("We hold that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents . . . reasonably suspect that the traveler is smuggling contraband in her alimentary canal.").

[6] *Riley v. California*, 573 U.S. 373, 396 (2014); *see United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013) (describing a forensic search of a laptop's hard drive as "essentially a computer strip search").

[7] U.S. Customs & Border Protection, CBP Directive No. 3340-049A (Jan. 4, 2018), https://www.dhs.gov/sites/default/files/publications/CBP%20Directive%203340-049A_Border-Search-of-Electronic-Media.pdf; *see* Rahul Mukhi & Britta Redwood, "New Rules for Searching Electronic Devices at the U.S. Border," Cleary Cybersecurity & Privacy Watch, https://www.clearycyberwatch.com/2018/02/new-rules-searching-electronic-devices-u-s-border/.

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.* As the First Circuit noted, there is a pending petition for a writ of certiorari before the Supreme Court as to whether the Fifth Amendment protects an individual from being compelled to disclose passwords to electronic devices

U.S. Immigration and Customs Enforcement ("ICE") has adopted analogous rules to govern its searches of electronic devices at the border "to ensure compliance with customs, immigration, and other laws enforced by ICE."[12]

District Court Holds that Border Searches of Electronic Devices Violates the Fourth Amendment

Alasaad involved eleven plaintiffs, ten U.S. citizens and one legal permanent resident, each of whose electronic devices had been searched at the border at least once. The plaintiffs filed suit in the United States District Court for the District of Massachusetts, asserting that the CBP and ICE guidelines violated the Fourth Amendment's protection against unreasonable searches and seizures and their First Amendment right to freedom of expression.[13] Plaintiffs alleged that the material on their devices seized by border officers included personal pictures of them and family members, confidential information related to their work in journalism, and privileged communications with their attorneys.[14]

On November 12, 2019, the district court held that both "basic" and "advanced" searches of electronic devices at the border violate the Fourth Amendment unless there is reasonable suspicion that the devices contain contraband.[15] The court first analyzed whether these border searches were "routine" or "non-routine," focusing on a traveler's privacy interest in the contents of his or her electronic devices and the intrusiveness of these searches. Highlighting the "breadth of intrusion into personal information" from a search of a person's electronic devices, the court found that both "basic" and "advanced" searches were non-routine and therefore required reasonable suspicion.[16] The court held that it was "unable to discern a meaningful difference between the two classes of searches," given that both would give the Government access to private pictures, prescription information, travel history, communications with counsel, location data, and browsing history.[17]

The court did, however, draw a distinction between "cursory" and "non-cursory" searches, defining the former 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."[18] A "cursory" search would fall within the border exception, and would not require articulable suspicion.[19]

The court granted declaratory judgment for the plaintiffs, holding that non-cursory "basic" and "advanced" searches of electronic devices violate the Fourth Amendment unless there is reasonable suspicion that the devices contain contraband.[20]

Having found in plaintiffs' favor on their Fourth Amendment claims, the court held that plaintiffs were not entitled to any further relief for their First Amendment claims.[21]

The First Circuit Reverses

On February 9, 2021, a unanimous panel of the First Circuit reversed, holding that the Government's policies allowing for "basic" and "advanced" searches without probable cause did not violate individuals' constitutional rights.[22]

The court first rejected plaintiffs' argument that border searches of electronic devices require probable cause and a warrant.[23] The court cited Supreme Court precedent dating back to 1886 holding that border searches fall within a specific exception to the warrant

when doing so may expose the individual to criminal prosecution, but that issue was not raised here. *Alasaad v. Mayorkas*, 2021 WL 521570, at *2 n.4.

[12] Immigration and Customs Enforcement Directive No. 7-6.1, Border Searches of Electronic Devices, https://dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

[13] *Alasaad v. Nielsen*, 419 F. Supp. 3d 142 (D. Mass. 2019).

[14] *Id*. at 148-50.

[15] *Id.* at 147-48, 173.

[16] *Id.* at 163-65.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.* at 173.

[21] *Id.* at 168-70.

[22] *Alasaad v. Mayorkas*, 2021 WL 521570, at *1.

[23] *Id.* at *4-6.

requirement.[24] Although the Supreme Court held in *Riley v. California* that the search incident to arrest exception to the warrant requirement does not extend to searches of cellphones, the First Circuit found *Riley* to be inapplicable in the context of border searches.[25] The court reasoned that, while searches incident to arrest are premised on protecting officers and preventing evidence destruction, border searches are focused on protecting the border.[26] Requiring a warrant for the latter "would hamstring the agencies' efforts to prevent border-related crime and protect this country from national security threats."[27]

The First Circuit then parted from the district court in holding that basic border searches are "routine" searches that need not be supported by reasonable suspicion.[28] While recognizing that basic searches of electronic devices may reveal a trove of sensitive personal information, the court held that these concerns were tempered by the fact that the searches occur at the border, where the 'Government's interest in preventing the entry of unwanted persons and effects is at its zenith.'"[29] The key distinction identified by the court from searches previously found to be non-routine, such as certain invasive body searches, is that basic border searches of electronic devices "do not involve an intrusive search of a person."[30] The court also based this aspect of its decision on the scope of a basic search, which is limited to data resident on an electronic device, rather than deleted or encrypted files.[31]

The court next rejected plaintiffs' argument that border searches of electronic devices must be limited to searches for contraband, holding that "[a]dvanced 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."[32] This aspect of the opinion creates a circuit split with the Ninth Circuit, which held that the border search exception is restricted in scope to searches for contraband.[33]

Plaintiffs' challenges to the Government's device detention policies fared no better. The First Circuit held that these policies permit detention of electronic devices for only a reasonable period, tracking the constitutionally-permitted standard.[34] The court noted that this holding would not foreclose future as-applied challenges if a plaintiff could show that detention was unreasonable under the specific applicable circumstances.[35]

Finally, the First Circuit held that the content-neutral border search policies do not facially violate the First Amendment.[36] The court rejected the argument that the presence of potentially expressive material on electronic devices should trigger a more searching standard of review, and explicitly did not foreclose a future as-applied First Amendment challenge "if CBP and ICE were targeting journalists or using border searches to pierce attorney-client privilege."[37]

[24] *Id.* at *4.
[25] *Id.* at *5. The court noted that this conclusion was consistent with "[e]very circuit that has faced this question." *Id.* (citing *United States v. Aigbekaen*, 943 F.3d 713, 719 n.4 (4th Cir. 2019); *United States v. Cano*, 934 F.3d 1002, 1015-16 (9th Cir. 2019); *United States v. Vergara*, 884 F.3d 1309, 1312-13 (11th Cir. 2018)).
[26] *Id.*
[27] *Id.*
[28] *Id.* at *6-7. The First Circuit observed that it was the first federal court of appeals to address this question in a civil action, but that its decision was consistent with the holdings of the Ninth and Eleventh Circuits in criminal cases. *Id.* at *7 (citing *Cano*, 934 F.3d at 1016; *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018)).
[29] *Id.* at *6 (quoting *Flores-Montano*, 541 U.S. at 152).
[30] *Id.* (emphasis in original).
[31] *Id.*
[32] *Id.* at *7-8.
[33] *Id.* at *8 (citing *Cano*, 934 F.3d at 1018).
[34] *Id.* at *8-9. The First Circuit did not specifically address the reasonableness of the detention of any of plaintiffs' devices, one of which was held for 56 days. *Alasaad v. Nielsen*, 419 F. Supp. 3d at 150.
[35] *Alasaad v. Mayorkas*, 2021 WL 521570, at *9.
[36] *Id.* at *9-10.
[37] *Id.* at *10 & n.17.

Takeaways

The First Circuit's decision underscores that company executives entering and leaving the United States should not expect First or Fourth Amendment protections from "basic" searches of their electronic devices, and should take appropriate precautions to protect confidential and privileged information, particularly if they or their companies are under active or potential investigation by U.S. authorities.[38] This analysis applies whether travelers are U.S. citizens or non-citizens, although non-citizens may be subject to increased scrutiny at the border and potential risk of inadmissibility to the United States.

Travelers should consider implementing appropriate safeguards to mitigate the risk of disclosing confidential and privileged information through a "basic" manual search, including by:

- Using password protection for email and messaging services, as well as any confidential, privileged, or sensitive documents;
- Signing out of web-based services;
- Securing files with encryption; and
- Using electronic devices for travel that do not contain sensitive information.

Travelers should also be aware that any electronic devices they carry across the border may be subject to more intrusive "advanced" searches, which may give authorities access even to encrypted files.

The simplest and lowest risk option is not to carry any confidential information across the border, although that might not always be a practical option. Clients and lawyers alike should consider using a temporary smartphone or laptop computer (without sensitive information) while traveling, removing confidential information from their devices, disabling automatic syncing processes, logging off and disabling auto-password features, and turning off syncing of cloud services, among other measures.

Clients and lawyers should also be sure to assert any applicable privileges if an officer begins to search their electronic devices. The CBP and ICE policies require that officers who encounter information that is asserted to be protected by the attorney-client privilege or attorney work product doctrine must contact counsel from that agency and/or the appropriate U.S. Attorney's Office, who will ensure the separation of any privileged material from any information examined during a border search.[39]

For in-house counsel in particular, attorneys from all jurisdictions should consider their ethical obligations to protect privileged information when crossing the border. The New York City Bar Association recently issued an opinion on lawyers' ethical duties regarding U.S. border searches of electronic devices, which is instructive:

- A lawyer may disclose clients' confidential information only to the extent "reasonably necessary" to respond to a government agent's claim of lawful authority. Under the guidance of the formal opinion, a lawyer has an ethical obligation to first decline to provide access to client confidential information, to disclose only where there is no "reasonable, lawful alternative to disclosure," and then to limit the scope of disclosure to the extent possible.
- To the extent that any client confidential information is disclosed during a border

[38] For more information on preserving privilege when conducting an investigation or providing legal advice in a foreign jurisdiction, consult Cleary Gottlieb's Global Crisis Management Handbook, available at https://www.clearygottlieb.com/practice-landing/global-crisis-management.

[39] U.S. Customs & Border Protection, CBP Directive No. 3340-049A ¶ 5.2 (Jan. 4, 2018), https://www.dhs.gov/sites/default/files/publications/CBP%20Directive%203340-049A_Border-Search-of-Electronic-Media.pdf; Immigration and Customs Enforcement Directive No. 7-6.1, Border Searches of Electronic Devices ¶ 8.6(2)(b), https://dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

> search, lawyers must disclose this fact to their client to ensure that the client can take appropriate steps to protect its confidential information.[40]

Accordingly, in-house lawyers should limit the risks around traveling with confidential information that may be subject to search and, in the event a search is initiated, alert the authorities to his or her status as a lawyer and assert any applicable privileges. It may also be helpful for lawyers to bring proof of their bar membership while traveling to establish the existence of applicable privileges.

Time will tell whether the First Circuit's decision will be adopted nationwide or whether the Supreme Court will weigh in given the split with the Ninth Circuit. Nevertheless, given that the Government's current policies remain in effect, company executives and in-house counsel should continue to take steps to mitigate the risks set forth above.

…

CLEARY GOTTLIEB

[40] New York City Bar Association Committee on Professional Ethics, Formal Opinion 2017-5: An Attorney's Ethical Duties Regarding U.S. Border Searches of Electronic Devices Containing Clients' Confidential Information (May 9, 2018), https://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/formal-opinion-2017-5-an-attorneys-ethical-duties-regarding-us-border-searches-of-electronic-devices-containing-clients-confidential-information.