CLEARY GOTTLIEB

ALERT MEMORANDUM

Prosecution for Wiping Cellphone During Warrantless Customs Interrogation Highlights Risks at Border

August 26, 2026

On January 24, 2025, a U.S. citizen returning home from a vacation abroad was stopped at Atlanta International Airport and, when government agents attempted to seize his personal cellphone during a warrantless border search, he caused his phone's data to be wiped with a pre-installed software. In a novel development, federal prosecutors in Atlanta are now pursuing charges against the individual under a seldom-used statute for allegedly destroying property in order to prevent seizure. Specifically, when agents asked for his cellphone password, the individual provided a "duress password," which irreversibly wiped the device and prevented the agents from searching it. Prosecutors argue that the defendant's conduct amounts to criminal destruction of property under 18 U.S.C. § 2232.

This prosecution highlights the legal risks and uncertainty that even lawful entrants to the United States—including U.S. citizens—face when confronted by government interrogation or detention at borders and entry points. With this development, as well as the differing legal standards that have developed around the country in relation to border searches, it is more important than ever for individuals and organizations to understand their rights and obligations when entering the United States, including whether they are required to turn over or provide access to electronic devices that may contain sensitive, privileged, or confidential information.

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

New York

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

Joon H. Kim
+1 212 225 2950
jkim@cgsh.com

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

Elizabeth Hanft
+1 212 225 2150
ehanft@cgsh.com

I. Background

In January 2025,[1] a United States citizen was detained by federal authorities at Hartsfield-Jackson Atlanta International Airport upon returning home from a vacation in the Dominican Republic. During a customs interrogation, authorities seized the man's cellphone without a warrant. When asked to provide his device passcode, he entered what is known as a "duress passcode"—a code designed to wipe the contents of an electronic device when entered.

In November 2025, federal prosecutors in the Northern District of Georgia secured an indictment against the man under 18 U.S.C. § 2232, which criminalizes the "[d]estruction or removal of property to prevent seizure." Importantly, Section 2232 does not require the government to demonstrate that the destruction of property obstructed or was related to any official investigation—only that the destruction had the "purpose of preventing or impairing the Government's lawful authority to take such property," "before, during, or after any search or seizure of property." To date, the government has not publicly indicated whether the defendant was under investigation prior to his detention.

At a recent hearing, the defendant argued that his seizure was unlawful and that he was targeted because of his political activism in Atlanta. He also claimed that he was repeatedly denied access to a lawyer during his detention. The government argued that it possesses broad authority to search and seize property at U.S. borders and ports of entry because international travelers have not yet been authorized to enter U.S. soil and therefore are not entitled to the full protections against unreasonable search and seizure under the Fourth Amendment to the U.S. Constitution.

[1] While this arrest was over a year-and-a-half ago, it received little attention at the time until a recent article highlighting the incident appeared in *The New York Times*. See https://www.nytimes.com/2026/07/28/us/duress-password-phone-wipe-charge.htmlXX.

[2] U.S. Customs & Border Protection, CBP Directive No. 3340-049A (Jan. 4, 2018).

II. Customs and Border Patrol and ICE Guidelines for Searching Electronic Devices

In 2018, CBP announced updated guidelines differentiating "basic" searches (manual examination of a device's contents) from "advanced" searches (those using external equipment to review, copy, or analyze a device's contents).[2] Under these guidelines, a basic search may be performed without any basis for suspicion whatsoever, while an advanced search requires reasonable suspicion of criminal activity or a national security concern.[3] If a traveler declines to assist in opening a password-protected device, officers may temporarily detain or permanently seize the device.[4] U.S. Immigration and Customs Enforcement (ICE) has adopted analogous rules.[5] These guidelines apply equally to U.S. citizens and non-citizens.

In January 2026, U.S. Customs and Border Protection (CBP) released updated guidelines for border searches of electronic devices, which largely track the 2018 guidelines, including by providing that "[a]n officer may conduct a basic search of an electronic device with or without suspicion," subject only to minimal limitations.[6] One notable addition to the guidelines is a provision that instructs agents to conduct their searches "in accordance with applicable statutes, regulations, and judicial authorities", recognizing that "[a]dditional or different requirements may apply in certain jurisdictions."[7]

III. The Constitutionality of Searches of Electronic Devices at the Border

In recent years, courts have increasingly grappled with the unique privacy interests implicated by cellphones. In 2014, the Supreme Court in *Riley v. California*, took up the question, for the first time, of whether police

[3] *Id*. § 5.1.3.

[4] *Id*. § 5.3.3.

[5] Immigration and Customs Enforcement Directive No. 7-6.1, Border Searches of Electronic Devices.

[6] U.S. Customs & Border Protection, CBP Directive No. 3340-049A (Jan. 1, 2026) § 5.3.1.

[7] *Id*. § 2.9.

could search the contents of a cellphone without a warrant in a search incident to arrest. Recognizing that in the modern era, cellphones contain "the privacies of life," the Court held that absent case-specific exigent circumstances, police were required to obtain a warrant before searching an arrestee's phone.[8]

While guidance from the Supreme Court about warrantless searches incident to arrests is clear, the Court has yet to weigh in directly on the constitutionality of warrantless searches of electronic devices at the border. The question is whether the long recognized "border search" warrant exception is an exigent circumstance allowing the government to search cellphones at the border.

The border search exception is a powerful tool that the Court has repeatedly upheld as constitutional. In *United States v. Flores-Montano*, 541 U.S. 149 (2004), for example, the Court considered an appeal by an individual apprehended while allegedly smuggling drugs in a car across the U.S.-Mexico border. Customs inspectors had found over 81 pounds of marijuana after a warrantless search of the car's gas tank at a U.S. border checkpoint in California. At trial, the individual moved to suppress the drugs recovered from the gas tank arguing that he had a protected privacy interest in his vehicle and a divided Ninth Circuit panel agreed. The Supreme Court reversed the Ninth Circuit, holding that the government's interest in searching the car outweighed the man's privacy interest because "the government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[9] Though the decision suggested that the government's interest in protecting the border granted it exceedingly broad authority to search property, it did leave open the possibility that "some searches of property are so destructive as to require a different result[.]"[10]

Relying on *Flores-Montano* and similar cases, lower courts have accordingly almost universally adopted a broad interpretation of the "border search" warrant exception in the context of searches of electronic devices. In 2021 the First Circuit ruled in *Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021) that the government may conduct "basic" manual searches of electronic devices at the border without probable cause—or even reasonable suspicion. The court also held that even "advanced" searches using external equipment require neither probable cause nor a warrant, requiring only reasonable suspicion.

Since *Alasaad* was decided, other Circuits confronting this issue have generally agreed that the government may conduct "basic" searches of electronic devices at the border without a warrant or reasonable suspicion. The First, Fourth, Fifth, Seventh, and Eleventh Circuits have all affirmatively held that government authorities may lawfully seize and search electronic devices under the "border search" exception without reasonable or individualized suspicion.[11] Additionally, while the Eighth Circuit has yet to definitively rule that individualized suspicion is unnecessary for routine border searches, it has strongly implied that it is not.[12]

The Ninth Circuit also permits basic border searches without individualized suspicion, provided there is

[8] *Riley v. California*, 573 U.S. 373, 403 (2014).
[9] *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).
[10] *Id*. at 155.
[11] *United States v. Belmonte Cardozo*, --- F.4th ---, 2026 WL 2014649, at *7 (4th Cir. 2026) ("manual searches of cell phones at the border are routine border searches which don't require individualized suspicion"); *United States v. Castillo*, 70 F.4th 894, 898 (5th Cir. 2023) ("the government can conduct manual cell phone searches at the border without individualized suspicion"); *United States v. Mendez*, 203 F.4th 1303, 1310 (7th Cir.) ("manual searches of a traveler's electronic device are 'routine' border searches requiring no individualized suspicion."); *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018) ("We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property.").
[12] *United States v. Xiang*, 67 F.4th 895, 900 (8th Cir. 2023) (evaluating whether reasonable suspicion becomes required when a routine border search is extended into an "advanced search," where a cellphone was seized at the border and shipped to an FBI laboratory for forensic examination).

some "nexus" between the warrantless search and digital or physical contraband.[13]

IV. Divergent Authority in The Second Circuit

Although the vast majority of courts have ruled in favor of the government's expansive interpretation of its search and seizure authority at the border, two district courts in the Second Circuit have ruled that the warrantless search and seizure of electronic devices is unlawful absent a warrant or exigent circumstances.

In *United States v. Smith*, 673 F. Supp. 3d 381 (S.D.N.Y. 2023), an individual who was a U.S. citizen was detained at Newark airport after returning from Jamaica. The Department of Homeland Security's Investigations unit had been investigating the defendant for conspiracy relating to immigration offenses. Government agents seized and searched the man's cellphone and copied its contents without first obtaining a warrant. The defendant moved to suppress the evidence, arguing the warrantless search violated his Fourth Amendment rights. Judge Rakoff in the Southern District of New York agreed, suppressing the evidence and holding that the search and seizure of a cellphone is not a routine border search because "the government's interests in a warrantless search of a cell phone's data are . . . much weaker than its interests in warrantless searches of physical items, and a traveler's privacy interests in her cell phone's data are much stronger than her privacy interests in her baggage."[14] He therefore held that the government may not manually search or copy an American citizen's cellphone at the border without a warrant absent exigent circumstances.[15]

Similarly, in *United States v. Sultanov*, 742 F. Supp. 3d 258 (E.D.N.Y. 2024), Judge Morrison in the Eastern District of New York held that "the search of a cell phone at the border is a nonroutine search for Fourth Amendment purposes" and that therefore a warrant is required.[16]

While the courts in *Smith* and *Sultanov* held that a warrant is required, other courts in the Second Circuit have held otherwise, notably in *United States v. Huawei Technologies Co., Ltd.*, 18-CR-457 (AMD) (JAM), 2026 WL 2099020 (E.D.N.Y. 2026). In *Huawei*, Judge Donnelly in the Eastern District of New York declined to suppress evidence collected from laptops belonging to Huawei employees seized at Dallas-Fort Worth International Airport by customs agents pursuant to an ongoing investigation.[17] Judge Donnelly held that a warrant was not required in such circumstances, but implied that the government needed at least reasonable suspicion to search electronic devices under the border search exception.[18]

The Second Circuit is currently considering the government's appeal in *United States v. Smith*, and it remains to be seen whether it will affirm that decision—which would make the Second Circuit an outlier among the federal circuits of appeal on the issue.

V. Additional Constitutional Considerations

The Atlanta prosecution also implicates an unresolved question at the intersection of the Fifth Amendment and border searches: whether the government can compel a traveler to disclose a device passcode. The Fifth Amendment's privilege against self-incrimination protects individuals from being compelled to make

---

[13] *United States v. Cano*, 934 F.3d 1002, 1016 (9th Cir. 2019).

[14] *United States v. Smith*, 673 F. Supp. 3d 381, 395 (S.D.N.Y. 2023).

[15] *Id*. at 396.

[16] *United States v. Sultanov*, 742 F. Supp. 3d 258, 284 (E.D.N.Y. 2024). Although the Court found that the warrantless search of the defendant's phone at the border was unconstitutional, it nonetheless declined to suppress evidence obtained from a later forensic search of the phone after a warrant had been obtained because the later search was conducted upon the "objectively reasonable" reliance on a warrant issued in good faith. *Id*. at 299.

[17] *United States v. Huawei Technologies Co., Ltd.*, 18-CR-457 (AMD) (JAM), 2026 WL 2099020, at *10 (E.D.N.Y. 2026)

[18] *Id*. at *9.

"testimonial" communications that could incriminate them.[19] In recent years, courts have frequently confronted the question of whether the compelled provision of a passcode or biometric data—such as a fingerprint or face ID—is testimonial in nature.

While there is no clear circuit consensus, the majority of courts that have considered whether provision of a passcode is testimonial have concluded that it is. For example, in *United States v. Guia-Lopez*, No.22-50234, 2023 WL 5236764 (5th Cir. Aug. 15, 2023), a man crossing the United States border was detained by border patrol agents. Despite invoking his *Miranda* rights, the agents continued questioning the individual, who eventually provided them with the password for his phone. The Fifth Circuit affirmed the district court's decision to suppress the disclosure of the passcode itself holding that "asking [the defendant] to write down his password was a Fifth Amendment violation because th[e] request . . . result[ed] in testimonial evidence that implicitly showed [the defendant's] ownership of the phone."[20] Ultimately, however, despite concluding that a Fifth Amendment violation had occurred, the court ruled that the contents of the phone were nevertheless admissible because the evidence obtained through examining the contents of the phone did not stem from the "exploitation" of the underlying constitutional violation.[21] District courts considering the issue have generally also determined that providing a passcode is testimonial.[22]

Although there is growing consensus among courts that communicating a passcode is testimonial, courts are more likely to determine that providing biometric data is not. For example, in *United States v. Payne*, 99 F.4th 495, (9th Cir. 2024), the Ninth Circuit affirmed the denial of a defendant's motion to suppress evidence obtained after police officers had forced him to use his thumb print to unlock his phone. In so holding, the court differentiated between the act of providing a passcode thereby revealing the contents of a person's mind, and the purely physical act of pressing a thumb to a scanner.[23] Ultimately, the court held that "the use of [a] thumb to unlock [a] phone was not a testimonial act and the Fifth Amendment does not apply[.]"[24] Although there is little consensus, district courts in other Circuits likewise often hold that providing biometric data is not testimonial.[25]

Taken together, these decisions suggest that refusal to provide a passcode is likely to be protected by the Fifth Amendment privilege against compelled disclosure, while the provision of biometric data such as a finger print or face ID may not be. However, it should be noted that neither the Supreme Court, nor the majority of Circuit courts have weighed in on these distinctions, so the application of these doctrines will depend on the context and the court.

VI. Takeaways

The recent Atlanta prosecution and the current state of the law have significant implications for company

[19] *See United States v. Hubbell*, 530 U.S. 27, 34, (2000).
[20] *Id*. at *6.
[21] *Id*. at *7.
[22] *See, e.g., United States v. Gogic*, 770 F.Supp.3d 529, 538 (E.D.N.Y. 2025) ("the revelation of a passcode from a suspect's mind or memory is testimonial in character."); *United States v. Shvartsman*, 722 F. Supp. 3d 276, 316 (S.D.N.Y. 2024) ("[Defendant]'s articulation of the phone passcode—like the 'vast majority of verbal statements'—was 'testimonial.' and the "foregone conclusion" doctrine did not apply"); *United States v. Booker*, 561 F.Supp.3d 924, (S.D. Cal. 2021); *United States v. Hearst*, No. 1:18-cr-054-RWS-AJB, 2022 WL 16832834, at *10 (N.D.G.A. Mar. 10, 2022) (collecting cases).
[23] *Id*. at 511.
[24] *Id*. at 513.
[25] *See, e.g.*, *Matter of Search of [Redacted] Washington, District of Columbi*a, 317 F. Supp. 3d 523, 535 (D.D.C. 2018); *In re Search Warrant Application for [Redacted Text]*, 279 F.Supp.3d 800, 804 (N.D. Ill. 2017); *United States v. Patel*, 25 Cr. 00173 (VM), 2026 WL 849850, at *5 (S.D.N.Y. Mar. 27, 2026) (observing that neither the court nor the defendant could identify "any case in the Second Circuit supporting the contention that the compelled use of biometrics to unlock a device is a testimonial act that facially violates the Fifth Amendment.")

executives, employees, attorneys, and other individuals entering and leaving the United States.

Geographic Variation in Legal Protections

Travelers should be aware that the level of legal protection a traveler is entitled to may vary depending on the jurisdiction of their port of entry. However, given the conflicting legal regimes among Circuits and the generally broad interpretation of government power to search and seize electronic devices at the border, travelers should assume that the border search exception to the Fourth Amendment's warrant requirement will apply and anticipate that their electronic devices may be subject to search without probable cause or a warrant.

Heightened Risk from Protective or Duress Mechanisms

The Atlanta indictment illustrates that employing protective or "duress" mechanisms designed to destroy, wipe, or obstruct government access to data on electronic devices materially increases legal risk. The defendant in the Atlanta case faces federal criminal charges under 18 U.S.C. § 2232 solely for activating a mechanism that wiped his phone's contents after the device was seized. Section 2232 does not require the government to show that the destruction was related to any pending investigation or that the data destroyed was itself evidence of a crime—only that the act was intended to "prevent[] or impair[] the Government's lawful authority to take such property."

Travelers should understand that the government's seizure of an electronic device at the border is likely to be deemed lawful. Accordingly, any subsequent act that destroys, alters, or obstructs access to data on that device—whether through a duress passcode, remote wipe capability, or other mechanism—could form the basis of a federal criminal prosecution. The prudent course is to leave laptops and cellphones with sensitive data at home and not to use "duress passwords," or similar software on electronic devices in connection with border crossings.

Recommended Safeguards

In light of the foregoing, travelers should not expect Fourth or Fifth Amendment protection from "basic" border searches of their electronic devices and should take appropriate precautions to protect confidential and privileged information before crossing the border. This guidance applies to U.S. citizens and non-citizens alike, although non-citizens may face increased scrutiny and potentially fewer protections.

Travelers should consider implementing the following safeguards to mitigate the risk of exposing confidential and privileged information through a border search:

— Using password protection for email and messaging services, as well as for any confidential, privileged, or sensitive documents stored on the device;

— Signing out of web-based services and disabling auto-login and auto-password features; [as per below, perhaps consider disabling "facial recognition" unlocking functionality]

— Securing sensitive files with encryption;

— Leaving devices with sensitive information at home or using a dedicated travel device that does not contain sensitive information;

— Removing confidential or privileged information from devices before travel;

— Politely declining to provide a passcode or biometric access if asked, while anticipating that the device will likely be detained or seized; and disabling biometric unlock features (facial recognition, fingerprint) before reaching the border, as biometric access may be physically compelled without the same Fifth Amendment protections that may apply to memorized passcodes.

— Disabling automatic syncing processes and turning off cloud synchronization to prevent remote access to cloud-stored data.

Asserting Privilege and Ethical Obligations of Counsel

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

In-house counsel and outside attorneys from all jurisdictions should carefully consider their ethical obligations to protect privileged information when crossing the border. For example, the New York City Bar Association's Formal Opinion 2017-5 on lawyers' ethical duties regarding U.S. border searches of electronic devices 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 search, lawyers must promptly disclose this fact to their client so that the client can take appropriate steps to protect its confidential information.

Accordingly, lawyers should be mindful of the potential risks around traveling with confidential information that may be subject to search. In the event a search is initiated, lawyers should alert the authorities to their status as counsel and assert any applicable privileges. It may be helpful for lawyers to carry proof of bar membership while traveling to establish the existence of applicable privileges.

Conclusion

The recent Atlanta case highlights the government's evolving enforcement posture at U.S. borders. Travelers, company executives, and counsel should take proactive steps to ensure that sensitive and privileged information is not carried across the border and should refrain from using device-wiping or data-destruction mechanisms which could lead to criminal liability. Given the unsettled and rapidly evolving nature of this area of law, organizations and individuals who regularly travel internationally should carefully consider efforts to mitigate the risks associated with border crossings with sensitive material by consulting with experienced counsel.

…

CLEARY GOTTLIEB