LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Rethinking Corporate Travel Rules After Device Search Cases

By **Nicola Hanna and Sam Raymond** (August 19, 2026, 5:41 PM EDT)


Nicola Hanna


Sam Raymond

This summer, a decision by a federal judge in New York and pending developments in a first-of-its-kind federal prosecution in Georgia, have sharpened the stakes for corporations whose employees carry electronic devices across U.S. borders.

On June 18, U.S. District Judge Ann Donnelly in the U.S. District Court for the Eastern District of New York ruled in U.S. v. Huawei Technologies Co. Ltd. that the border search exception to the Fourth Amendment justified the warrantless seizure and subsequent search of company laptops carried by a corporate employee.

The seizures took place back in February 2018 and April 2018, when federal agents twice stopped the employee at Dallas-Fort Worth International Airport as he returned from overseas, without a warrant. The court's ruling confirms the breadth of the government's border search authority.

Meanwhile, in a case now pending in the U.S. District Court for the Northern District of Georgia — U.S. v. Tunick — federal prosecutors have charged traveler Samuel Tunick with a felony for his response to a warrantless border inspection. In January 2025, federal agents at Hartsfield-Jackson Atlanta International Airport stopped the traveler and insisted he provide the passcode to his phone.

The code Tunick provided did not unlock the device. Instead, the code triggered a feature that erased all data on the phone. In November 2025, a grand jury indicted him under a rarely invoked statute criminalizing the destruction of property to prevent its seizure, in what appears to be the first prosecution of its kind.

The case remains pending, with a suppression hearing conducted this summer, and how the matter is resolved will shape what travelers can lawfully do when agents demand access to their devices.

Together, the two cases underscore how little protection corporate personnel have at the border. As reflected in Huawei, law enforcement officers at the border may search and seize electronic devices without a warrant and, in most circuits, without probable cause.

Though Tunick may be an outlier, it does signal that certain efforts to resist a seizure at a border checkpoint could carry criminal consequences. And the law is still moving: appeals raising the warrant question are awaiting decision in the U.S. Court of Appeals for the Second Circuit.

This article summarizes the law, unpacks those cases, and offers considerations for corporations that are or may become subjects of investigation whose employees cross U.S. borders.

Legal Backdrop: The Border Search Exception

The Fourth Amendment ordinarily requires that the government obtain a warrant supported by probable cause before agents may search or seize private property. At the border, however, the standard is different.

The U.S. Supreme Court has long held that "searches at our borders without probable cause and without a warrant are nonetheless reasonable," as noted in U.S. v. Ramsey in 1977.[1] Even intrusive border searches may be performed without a warrant or probable cause, so long as agents have reasonable suspicion of criminal conduct.[2]

Courts have divided on how these principles apply to electronic devices carried by travelers.

In 2019, the U.S. Court of Appeals for the Ninth Circuit — which covers major transit hubs like Los Angeles and San Francisco International Airports — held in U.S. v. Cano that manual searches of electronic devices require no suspicion at all, but that forensic examination requires reasonable suspicion, meaning suspicion that the device contains digital contraband.[3]

In 2018, the U.S. Court of Appeals for the Eleventh Circuit — which covers Atlanta and in the jurisdiction of which Tunick arises — held in U.S. v. Touset that no suspicion whatsoever is required for any border searches of electronic devices, whether manual or forensic.[4]

The U.S. Court of Appeals for the Fourth Circuit, in U.S. v. Aigbekaen in 2019, held that forensic searches at the border require agents to "have individualized suspicion of an offense that bears some nexus to the border search exception's purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband."[5]

Huawei illustrates how the border search doctrine, and the various cases interpreting the doctrine, operates with respect to a corporation. Agents stopped a Huawei employee at Dallas-Fort Worth International Airport twice, seized company-owned laptops he was carrying, and forensically imaged them — all without a warrant — while a government investigation of the company was already underway.

The Eastern District of New York held that the border search exception applied to both the warrantless seizures and the forensic imaging of the devices.[6] The court further held that the employee's apparent authority to consent to the searches defeated Huawei's internal information security policies, which prohibited employees from disclosing corporate data or credentials to third parties.

And the court expressly rejected the warrant requirement that other district courts within the Second Circuit had adopted for border searches of cellphones.[7]

The landscape in the Second Circuit may yet shift. Four appeals involving warrantless border device searches are currently pending before the Second Circuit, including U.S. v. Alisigwe, U.S. v. Kamaldoss, U.S. v. Smith and U.S. v. Robinson.[8]

Unlocking Password-Protected Devices in Light of Tunick

The border search exception may authorize law enforcement to seize and search electronic devices, but modern encryption can make such searches difficult in practice.

For devices protected by passcodes, courts have reached differing results on whether law enforcement can compel the traveler to provide the code.[9]

Against that backdrop, the charges in Tunick raise the stakes for password compulsion at the border. According to the charges and court filings, Tunick was referred to secondary inspection at Hartsfield-Jackson Atlanta International Airport, where agents insisted he provide a passcode to his phone.

According to Tunick, the agents showed neither a warrant to seize the phone, nor compulsory process to demand he give the passcode. Ultimately, he provided a passcode, but the code did not unlock the phone — it wiped all data. His phone ran GrapheneOS, an alternative operating system that can be configured to erase a device when a designated code is entered.

Based on this deletion of data, the grand jury indicted him under Title 18 of the U.S. Code, Section 2232(a), which criminalizes knowingly destroying or disposing of property to prevent its seizure by the government.[10]

Notably, prosecutions under Section 2232 are rare, and the statute's traditional applications have been in the forfeiture context — defendants dissipating, transferring or destroying forfeitable assets, or dumping contraband, ahead of an anticipated seizure.[11] It has very rarely, if ever, been used to criminalize destroying electronic data to prevent seizure.

Under the government's theory in Tunick, the data on a phone is property, and its destruction during a warrantless border inspection is obstruction of a seizure. The case presents novel questions, some of which are of first impression: whether intangible data qualifies as property under Section 2232; whether the attempted seizure by the government was lawful under the border search exception and whether that matters; whether Tunick acted knowingly when law enforcement insisted he provide a code; and whether his provision of the passcode was testimonial.

However those questions are resolved, the indictment itself carries a message: The U.S. Department of Justice appears willing, at least in some cases, to charge travelers who take steps to place their data beyond the government's reach during a border inspection.

Implications for Corporate Travel Programs

For corporations whose employees cross U.S. borders, the Huawei and Tunick cases indicate several important considerations.

First, wipe and auto-delete features could be highly risky, if not criminal, at the border. Whatever the outcome of the pending charges in Tunick, a felony indictment is a severe consequence for an employee and a serious event for an employer — particularly one already under investigation.

Before relying on electronic features to protect data, corporations should weigh the risk that the operation of these features during a seizure could be treated as criminal.

Second, corporate policies do not travel with the device. Under Huawei's apparent-authority holding, an employee who hands over passwords and consents to a search can validate that search as against the company, no matter what internal policies provide.

The court reasoned that agents need not familiarize themselves with an employer's policies, and that a company that permits an employee to travel internationally with corporate devices assumes the risk that he will consent. Login banners and signed information security policies were not enough.

Corporations should consider training traveling employees to state clearly that they lack the authority to consent to a search of corporate data, and that company counsel should be contacted.

Third, timing is crucial. The charges in Tunick signal that destroying data during an inspection is potentially criminal. Minimizing data before travel, by contrast, should remain lawful preparation.

Companies should consider providing traveling employees with clean devices for border crossings, cloud-only access with credentials not carried on the device, and standing data minimization policies documented well in advance.

Such efforts could reduce what is exposed at the border and may rebut any suggestion that a lightly loaded device reflects knowing destruction rather than routine practice.

Conclusion

Several developments bear watching: the outcome of Tunick, including whether Section 2232's application to data survives; the four pending Second Circuit appeals; and whether the deepening disagreement among the circuits will eventually draw the Supreme Court to the question of border device searches.

In the meantime, the uncertainty in the law counsels that corporations should prepare now — before their employees reach the border and potentially have devices seized and searched, not after.

Nicola Hanna is a partner and co-chair of the global white collar defense and investigations practice group at Gibson Dunn & Crutcher LLP. He previously served as the U.S. attorney for the Central District of California.

Sam Raymond is of counsel at the firm. He previously served as an assistant U.S. attorney for the Southern District of New York.

[1] United States v. Ramsey, 431 U.S. 606, 619 (1977) (noting this history is "as old as the Fourth Amendment itself").

[2] United States v. Montoya de Hernandez, 473 U.S. 531, 541 — 42 (1985).

[3] United States v. Cano, 934 F.3d 1002, 1007, 1018 — 21 (9th Cir. 2019).

[4] United States v. Touset, 890 F.3d 1227, 1231 — 33 (11th Cir. 2018).

[5] United States v. Aigbekaen, 943 F.3d 713, 721 (4th Cir. 2019).

[6] United States v. Huawei Technologies Co., No. 18-CR-457 (AMD) (JAM), 2026 WL 2099020 (E.D.N.Y. June 18, 2026, unsealed July 21, 2026).

[7] See, e.g., United States v. Smith, 673 F. Supp. 3d 381 (S.D.N.Y. 2023); United States v. Sultanov, 742 F. Supp. 3d 258 (E.D.N.Y. 2024).

[8] United States v. Alisigwe, No. 24-960 (2d Cir. argued Mar. 28, 2025); United States v. Kamaldoss, No. 24-824 (2d Cir. argued Mar. 31, 2025); United States v. Smith, No. 24-1680 (2d Cir. argued June 24, 2025); United States v. Robinson, No. 25-1428 (2d Cir. argued Apr. 14, 2026).

[9] Compare In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012) (holding that provision of a passcode is testimonial and that compelled disclosure violated the Fifth Amendment where the government could not show it already knew what files were on the devices) with United States v. Smith, 706 F. Supp. 3d 404, 408 (S.D.N.Y. 2023) (compelled disclosure does not violate the Fifth Amendment, so long as the government can independently show the phone belonged to the person and that the person knew the password).

[10] United States v. Tunick, No. 25 Cr. 499 (N.D. Ga.).

[11] See, e.g., United States v. Harmon, No. 21-cr-00433 (D.D.C.); United States v. Switlyk, No. 25-12595, 2026 WL 810131 (11th Cir. Mar. 24, 2026); United States v. Kock, 66 F.4th 695, 704 (8th Cir. 2023).