

Open Issues After 2nd Circ.'s Airport Phone Search Ruling

By **Brendan Quigley and Frank Kratovil** (October 27, 2026)

"Can they search my phone at the airport?"

White collar defense attorneys and in-house counsel often hear this question from clients whose conduct may be under government scrutiny, even when the client is not personally suspected of wrongdoing, and whose ongoing job and personal responsibilities require overseas travel.

On Sept. 17, in *U.S. v. Alisigwe*, the U.S. Court of Appeals for the Second Circuit held that federal officers may manually search a traveler's cellphone at the border — including an international airport — without a warrant, probable cause or reasonable suspicion.[1]

However, the court expressly left open whether more sophisticated forensic examinations of a cellphone may require individualized suspicion of wrongdoing.[2]

Although *Alisigwe* clarifies the scope of border agents' authority to conduct manual cellphone searches at ports of entry inside the Second Circuit, significant questions remain about more wide-ranging cellphone searches at the border, both in the Second Circuit and across the country.



Brendan Quigley



Frank Kratovil

Background

The defendant in the case, Chinwendu Alisigwe, came under investigation for suspected use of fraudulent passports and identity theft.[3]

In 2019, as Alisigwe returned to the U.S. from a trip abroad, customs officers at John F. Kennedy International Airport in New York stopped him and instructed Alisigwe to unlock his cellphone.[4] An "officer then scrolled through Alisigwe's cellphone and used his own cellphone to photograph images contained in Alisigwe's photo gallery." [5] The "gallery contained images of other people's names, birthdates, and social security numbers as well as bank account information and addresses." [6]

More than two years later, as Alisigwe returned from another trip abroad, law enforcement again stopped him at JFK and "again manually reviewed his cellphone by scrolling through it and taking photographs." [7] They "photographed a WhatsApp message in which Alisigwe asked a co-conspirator whether he had received '[a]nything for' an individual whose identity Alisigwe had stolen." [8]

Prosecutors eventually charged Alisigwe with federal crimes relating to alleged bank fraud and identity theft. The U.S. District Court for the Southern District of New York denied his motion to suppress the evidence obtained from the two searches of his cellphone at JFK, finding law enforcement officers had sufficient suspicion of criminal activity to search the phone. Alisigwe proceeded to trial, and the jury convicted him in late 2023. He then appealed.

The Second Circuit Decision

In its Sept. 17 decision, the Second Circuit affirmed Alisigwe's conviction. The majority opinion, joined by two members of the three-judge panel, went further than the district court, holding that no individualized suspicion was required.

By way of background, the Fourth Amendment to the U.S. Constitution generally prohibits searches of property without a search warrant. A search warrant generally requires a judicial determination that there is probable cause to believe evidence of a crime will be found in the place to be searched.

In 2014, the U.S. Supreme Court held in *Riley v. California* that the exception for searches incident to arrest exception generally does not permit officers to search the digital contents of a cellphone without a warrant.[9]

However, case law has also recognized exceptions to the warrant requirement, including the so-called border-search exception. As the Alisigwe court observed, the "longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself." [10] It explained that the "border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." [11]

In addition, the decision noted that case law has recognized that some kinds of searches may be permissible under a showing of reasonable suspicion, a standard that is lower than probable cause but that still requires law enforcement to articulate "'a particularized and objective basis' for suspecting" criminal wrongdoing. [12]

The Second Circuit majority held that the border-search exception applied to the searches of Alisigwe's phone, rejecting both his argument that *Riley* required a warrant issued upon probable cause, and the district court's ruling — as well as one judge's concurring opinion, discussed more below — that reasonable suspicion was required.

The court noted that, "[u]nder our precedents, no suspicion is required before the government searches a traveler's property at the border." [13] Property searches "are made reasonable by that person's decision to enter this country," the court added. [14]

The majority did recognize that reasonable suspicion is required for nonroutine searches of a person, as opposed to property, at the border. But it explained that "the label 'non-routine' should generally be reserved for intrusive border searches of the person (such as body-cavity searches or strip searches), not belongings." [15]

That distinction resolved the issue for the majority. "Because a cellphone is property," not part of a person, the court concluded, "our precedents establish that the government does not need to have reasonable suspicion before searching a traveler's cellphone at the border." [16]

The court also rejected Alisigwe's argument that *Riley*, which emphasized the privacy interests associated with cellphones, mandated a warrant. [17] The Second Circuit acknowledged that "cellphones contain 'vast quantities of personal information'" and "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." [18]

But the court emphasized that "Riley did not address the border-search exception." [19] Riley concerned searches incident to arrest, which are justified by the risks of "harm to officers and destruction of evidence." [20] The border-search exception, by contrast, serves the government's broader "interest in preventing the entry of unwanted persons and effects," according to the court. [21]

The court ultimately held that Riley did "not alter the precedents that define the scope of the border-search exception," and that a search of a traveler's property at the border, including a cellphone, may be conducted without suspicion. [22]

The majority, however, expressly limited its decision to manual searches, i.e., a law enforcement officer's physical review of a cellphone. The court declined to "decide whether the use of 'sophisticated forensic search methods,' such as 'the off-site forensic analysis of the phone's data,' might qualify as a nonroutine search requiring reasonable suspicion." [23]

U.S. Circuit Judge Eunice C. Lee concurred in the judgment, but disagreed with the majority's conclusion that manual cellphone searches are routine and require no individualized suspicion. Emphasizing the volume and sensitivity of information stored on modern cellphones, she argued that treating a cellphone like ordinary property "denies a fundamental reality of the modern cellphone — it is not a suitcase." [24]

Case Law in Other Circuits and a Pending Cert Petition

The Second Circuit's decision in *Alisigwe* aligns with decisions of the U.S. Courts of Appeals for the First, Fourth, Fifth, Seventh, Ninth, Tenth and Eleventh Circuits, all of which have held that manual searches of cellphones at the border do not require individualized suspicion. [25]

Beyond that, however, there is a fair amount of disagreement among the circuits.

As to computer-aided, forensic searches of cellphones, two circuits — the Fourth and the Ninth — have held that individualized suspicion is required, and one, the Eleventh Circuit, has held that it is not. [26] The Fifth, Eighth and Tenth Circuits have also upheld warrantless forensic searches where officers possessed reasonable suspicion, but have declined to decide whether such suspicion was constitutionally required. [27]

The circuits also differ over what agents may look for on a phone if they are relying on the border-search exception, as opposed to getting a warrant. In *Alisigwe*, the Second Circuit, citing the government's "broad authority to control who and what enters the country," allowed agents to manually search a phone without a warrant for "evidence of criminality," not just evidence of border offenses. [28]

In contrast, the Fourth Circuit held in its 2019 *U.S. v. Aigbekaen* decision that such a warrantless search must look only for evidence of "an offense that bears some nexus to the border search exception's purposes." [29]

Similarly, the Ninth Circuit held that same year in *U.S. v. Cano* that warrantless forensic cellphone searches at the border require reasonable suspicion and that any search "must be limited in scope to a search for digital contraband," not evidence of crimes generally. [30]

At least some of these disagreements may soon reach the Supreme Court. An August petition for a writ of certiorari in *Anibowei v. Blanche* challenges the constitutionality of U.S.

Customs and Border Protection and U.S. Immigration and Customs Enforcement directives permitting border agents to conduct manual searches of travelers' electronic devices without a warrant or reasonable suspicion, and to conduct forensic searches without a warrant.[31]

The Supreme Court has requested a response from the government by Nov. 30, but has not yet decided whether to grant review.

Practical Implications

Alisigwe underscores border agents' broad authority to conduct routine manual cellphone searches at ports of entry. In the Second Circuit, to conduct a manual search, agents need neither a warrant nor reasonable suspicion that a traveler has committed a crime or that the cellphone contains evidence of wrongdoing.

As noted, the Second Circuit left open the possibility that a higher standard of suspicion would be required for more intrusive, computer-aided forensic searches of cellphones. Nor did it resolve whether agents may access cloud-based data without a warrant. These issues may be litigated in future cases.

The circuits disagree about whether forensic border searches require individualized suspicion, meaning other jurisdictions may reach differing conclusions on similar claims that implicate these issues. The Fourth and Ninth Circuits require individualized suspicion for forensic searches, while the Eleventh Circuit does not. At the same time, reasonable suspicion is a relatively low bar and does not require a warrant.

The border-search exception applies to international border crossings and their functional equivalents, including international airports. Notably, the general consensus in the case law supports applying the border-search exception to both inbound and outbound travel.[32] The border-search exception does not, however, apply to domestic flights.

Clients and companies whose personnel travel internationally may wish to consider what sensitive information is stored locally on devices used for international travel.

Any measures to limit information carried during international travel should account for applicable preservation and document-retention obligations — including litigation holds, regulatory recordkeeping requirements and internal record-management policies — by ensuring that any materials required to be preserved are preserved, possibly via the use of shared drives or different media than the device used for travel, if that kind of preservation is deemed appropriate under the circumstances.

Companies and travelers should also evaluate whether to enable auto-delete or similar features. If these features are unintentionally triggered during a border search, that could invite additional government scrutiny.

In *U.S. v. Tunick*, federal prosecutors charged a traveler last year in the U.S. District Court for the Northern District of Georgia with destruction of evidence after he allegedly provided border officers with a passcode that caused his phone's contents to be deleted.[33]

The prosecution illustrates the potential legal consequences of data-deletion measures during a border inspection, even as the law governing compelled access to electronic devices continues to develop.

Brendan F. Quigley is a partner at Baker Botts LLP. He previously served as an assistant U.S. attorney in the Southern District of New York.

Frank Kratovil is an associate at Baker Botts.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] United States v. Alisigwe, --- F.4th ----, No. 24-960, 2026 WL 2751713 (2d Cir. Sept. 17, 2026).

[2] Id. at *11 n.9.

[3] Id. at *1.

[4] Id. at *3.

[5] Id.

[6] Id.

[7] Id.

[8] Id.

[9] Riley v. California, 573 U.S. 373, 403 (2014) ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple — get a warrant.").

[10] Alisigwe, 2026 WL 2751713, at *1 (quoting United States v. Ramsey, 431 U.S. 606, 619 (1977)).

[11] Id. (quoting Ramsey, 431 U.S. at 620).

[12] See, e.g., D.C. v. R.W., 608 U.S. 22, 25 (2026).

[13] Alisigwe, 2026 WL 2751713, at *2 (citing United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006)).

[14] Id. (quoting Irving, 452 F.3d at 123).

[15] Id. (quoting United States v. Levy, 803 F.3d 120, 123 n.3 (2d Cir. 2015)).

[16] Id.

[17] Id. at *7.

[18] Id. at *8 (quoting Riley, 573 U.S. at 386, 393).

[19] Id. at *7.

[20] Id. (quoting *Riley*, 573 U.S. at 386).

[21] Id. at *8 (quoting *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004)).

[22] Id. at *11.

[23] Id. at *11 n.9 (quoting *United States v. Kolsuz*, 890 F.3d 133, 140, 146 n.5 (4th Cir. 2018)).

[24] Id. at *11 (Lee, J., concurring in the judgment).

[25] See *Alasaad v. Mayorkas*, 988 F.3d 8, 18-19 (1st Cir. 2021) ("Basic border searches are routine searches and need not be supported by reasonable suspicion."); *United States v. Belmonte Cardozo*, 181 F.4th 461, 464 (4th Cir. 2026); *United States v. Castillo*, 70 F.4th 894, 898 (5th Cir. 2023); *United States v. Mendez*, 103 F.4th 1303, 1308-10 (7th Cir. 2024); *United States v. Cano*, 934 F.3d 1002, 1007 (9th Cir. 2019); *United States v. Williams*, 942 F.3d 1187, 1190 (10th Cir. 2019); *United States v. Touse*, 890 F.3d 1227, 1233 (11th Cir. 2018).

[26] Compare *Kolsuz*, 890 F.3d at 144 ("a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion") and *Cano*, 934 F.3d at 1007 (holding that "'reasonable suspicion' in this context means that officials must reasonably suspect that the cell phone contains digital contraband") with *Touse*, 890 F.3d at 1231 ("[T]he Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border.").

[27] *Malik v. United States Dep't of Homeland Sec.*, 78 F.4th 191, 201 (5th Cir. 2023); *United States v. Xiang*, 67 F.4th 895, 900-01 (8th Cir. 2023); *Williams*, 942 F.3d at 1190.

[28] *Alisigwe*, 2026 WL 2751713, at *2.

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

[30] *Cano*, 934 F.3d at 1007.

[31] Petition for a Writ of Certiorari, *Anibowei v. Blanche*, No. 26-208 (U.S. Aug. 14, 2026).

[32] See, e.g., *United States v. Beras*, 183 F.3d 22, 26 (1st Cir. 1999) (collecting cases).

[33] Indictment, *United States v. Tunick*, 25 Cr. 499 (N.D. Ga. Nov. 17, 2025).