ALM | LAW.COM

New York Law Journal

WHITE-COLLAR CRIME

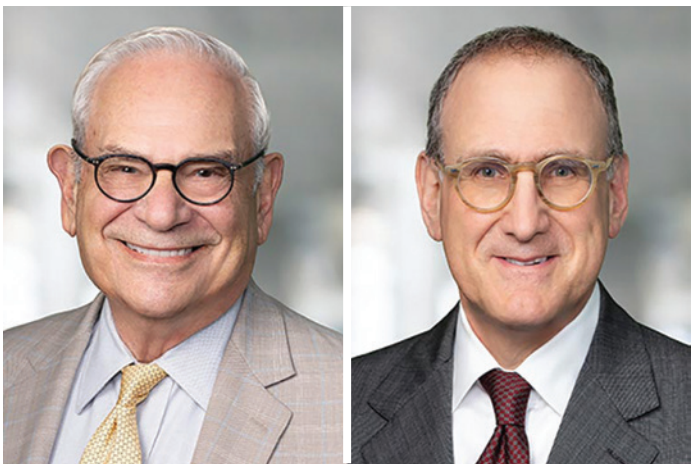
Border Searches and Electronic Data

By Elkan Abramowitz and Jonathan Sack

January 9, 2026

White-collar criminal cases commonly depend on documents, and these days documents such as emails and text messages are stored on electronic devices. We carry these devices when we travel, which means in practical terms that our data, including sensitive or even incriminating information, is subject to search when we enter or leave the United States.

The Supreme Court has created a legal framework of Fourth Amendment rights at the border which distinguishes between "routine" and "non-routine" searches. Routine searches do not require particularized suspicion about a traveler's conduct or possessions, whereas "non-routine" searches require at least "reasonable suspicion" to justify more invasive searches. While this distinction leaves uncertainty, such as what degree of intrusiveness is permitted in a non-routine search, the uncertainty is acute when it comes to data on electronic devices. Courts are grappling with such questions as (i) what may border officers examine in a routine search of a device, (ii) what may border officers examine in a non-routine search of a device, and (iii) what degree of suspicion—notably, reasonable suspicion or probable cause—is required for the review of electronic data.



Courtesy photos

Elkan Abramowitz, left, and Jonathan Sack.

In this article, we begin by summarizing Supreme Court case law and key Second Circuit decisions. We then discuss the different approaches taken by judges in the Second Circuit, focusing primarily on the recent decision by Judge Gary R. Brown, in the Eastern District of New York, *United States v. Walden*, 2025 WL 3154359 (E.D.N.Y. Nov. 12, 2025), which permitted the search and seizure of electronic data based on reasonable suspicion. The court disagreed with the approach taken in *United States v. Smith*, 673 F. Supp. 3d 381 (S.D.N.Y. 2023), in which Judge Jed S. Rakoff would require a search warrant under similar circumstances.

The Basic Framework

The Supreme Court has long recognized that the Fourth Amendment's "balance of reasonableness" is different at the border, such that routine searches of individuals and their property, whether entering or leaving the United States, "are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Government agents may conduct routine searches of travelers' bags and other personal items at the border or the Customs area of an international airport, which has been deemed the "functional equivalent of a border search," and may then seek to use the fruits of their search as evidence in criminal cases. *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973); see also *United States v. Ramsey*, 431 U.S. 606, 620-22 (1977).

The Supreme Court has taken a broad view of the "border search exception," for example, allowing the disassembling of an automobile gas tank without any suspicion. See *United States v. Flores-Montano*, 541 U.S. 149, 152-155 (2004); see also *United States v. Irving*, 452 F.3d 110, 123-24 (2d Cir. 2006). By comparison, the Supreme Court has required a showing of reasonable suspicion for what it has deemed more invasive "non-routine" searches. For example, the Supreme Court required reasonable suspicion to detain a traveler suspected of drug smuggling. See *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985); see also *United States v. Asbury*, 586 F.2d 973, 975-76 (2d Cir. 1978) (invasive searches, like strip searches, require reasonable suspicion).

In *Riley v. California*, 573 U.S. 373, 393 (2014), a non-border case, in which the Supreme Court addressed a warrantless search and seizure of a cell phone incident to arrest, has led to uncertainty about how cell phone and other digital data should be treated in various contexts. In *Riley*, the Supreme Court recognized that cell phones "differ in both a quantitative and a qualitative sense" from other personal belongings due to the amount of personal data they can contain, and held that the exception to the warrant requirement for searches incident to arrest does not apply to cell phone searches.

Courts have disagreed on how *Riley* should be applied to border searches, as we explain below.

Second Circuit Cases

In *United States v. Irving*, 452 F.3d 110, 123-24 (2d Cir. 2006), decided before *Riley*, the Second Circuit addressed a border search of "computerized information." Customs agents reviewed the contents of two computer diskettes and undeveloped film found in the luggage of an individual entering the United States who was suspected of possessing child pornography. Five years later, the individual was arrested and his home searched pursuant to a search warrant, which relied in part on the items found in his luggage.

The defendant made a motion to suppress evidence obtained from the border search, which the district court denied. The Second Circuit upheld denial of the motion without deciding whether the examination of the diskettes and undeveloped film constituted a "routine" or "non-routine" search because the Customs agents had reasonable suspicion, which was sufficient even if the search was deemed non-routine. *Irving*, 452 F.3d at 124 (citing *Asbury*, 586 F.2d at 975).

In *United States v. Levy*, 803 F.3d 120 (2d Cir. 2015), a defendant was returning to the United States to face potential criminal charges that arose from an alleged stock manipulation scheme. Customs and Border Protection (CBP) officers searched and photocopied a physical notebook in his possession. The search was conducted at the direction of the Drug Enforcement Administration, which was primarily responsible for the investigation since the alleged stock fraud scheme was uncovered

during a drug trafficking investigation. Less than 72 hours after the search, the defendant was indicted on charges of securities and wire fraud, based in part on incriminating material seized at the border. The defendant moved to suppress the photocopy of the notebook.

The district court found the search to be "non-routine" since "[t]he close reading and photocopying of an entrant's documents goes beyond the general searching one expects at a point of entry," but denied the motion because the government had reasonable suspicion that the defendant was engaged in stock fraud. *United States v. Levy,* 2013 WL 664712, at *12 (S.D.N.Y. Feb. 25, 2013). The Second Circuit affirmed, concluding that "[w]hether searching and copying the notebook here constitutes a 'routine' border search that could be conducted without reasonable suspicion is somewhat more debatable" (emphasis in original), but, consistent with the district court holding, the Second Circuit held that the investigation conducted prior to the search provided reasonable suspicion. The Second Circuit rejected the defendant's argument that border searches should be limited to crimes that "statute or regulation specifically authorizes [customs officers] to investigate." *Cf*. *United States v. Cano*, 934 F.3d 1002, 1018 (9th Cir. 2019).

'United States v. Walden'

In November, Brown upheld the search and seizure of a cell phone at JFK Airport based on reasonable suspicion. Homeland Security Investigations (HSI) agents stopped the defendant before he boarded an outbound flight to Italy and asked him and his wife for their electronic devices, which they produced, and for which they provided their passcodes on request. HSI had previously identified the defendant as a potential purchaser of Child Sexual Abuse Material (CSAM), which led to inclusion of the defendant's name in CBP computer systems that tracked his travel.

Initially an agent conducted a manual examination of defendant's phone, scrolling through a few screens and opening one application, which revealed several items relevant to the investigation, including a Cash App display name used for an account that had acquired CSAM, and applications the agent knew were used to distribute and conceal CSAM. The agent seized the phone, and a computer analyst created a forensic extraction of all the data on the phone. The data revealed CSAM and conversations regarding the purchase of CSAM. The defendant moved to suppress the material obtained from the stop and warrantless search at the airport.

Brown began by determining whether the initial manual search of the cell phone qualified as a routine border search. The defendant argued that all manual phone searches are non-routine, relying on *United States v. Sultanov*, 742 F. Supp. 3d 258 (E.D.N.Y. 2024), whereas the government contended that manual searches are categorically "routine," not requiring individualized suspicion, based on out of Circuit decisions. See, e.g., *United States v. Mendez*, 103 F.4th 1303, 1307 (7th Cir. 2024).

Brown sought a middle ground, explaining that "[t]he extent of a manual search can vary greatly, bearing on the appropriate analytical framework." Following *Levy*, Brown held that an examination and screenshot of a phone's "settings" screen, which could identify the phone as belonging to a certain individual, could properly be deemed "routine." However, the search of defendant's phone in this case went further and should be considered non-routine, requiring reasonable suspicion, due to its intrusiveness.

Next, Brown considered whether the agent had reasonable suspicion to justify the non-routine search of the phone under the *Levy* and *Irving* decisions discussed above. *Levy* permits customs agents to rely on information developed through an investigation by agents of a different agency, and *Irving* "sanctioned the non-routine search

of computer discs and undeveloped film based upon reasonable suspicion of the defendant's involvement in child sexual abuse." In this case, the agent had reasonable suspicion that the defendant had engaged in CSAM offenses, and the suspicion "continued to heighten" based on the initial examination of the phone. Brown held that both the initial manual examination of the phone and the subsequent forensic extraction from the device were supported by reasonable suspicion and did not require a search warrant. Brown's ruling is consistent with that of Judge Rachel P. Kovner in *United States v. Gavino*, No. 22-cr-136 (RPK), 2024 WL 85072 (E.D.N.Y. Jan. 7, 2024), which allowed the warrantless search of a cell phone based on reasonable suspicion at the border.

Earlier, in *Smith*, 673 F. Supp. 3d at 398,Rakoff, applying the *Riley* decision to border searches, stated that his "preferred rule" would require search warrants for phone searches at the border for American citizens, absent exigent circumstances. But the court did not ultimately suppress evidence on that basis because Rakoff found the good faith exception to the warrant requirement applicable. Judge Nina R. Morrison, consistent with Rakoff's reasoning, held that, in light of *Riley*, "the search of a cell phone at the border is a nonroutine search for Fourth Amendment purposes." *Sultanov*, 742 F. Supp. 3d at 284.

Brown disagreed with *Riley's* applicability to border searches and declined to find a probable cause and warrant requirement, which is consistent with the rule in the majority of circuits. See, e.g., *Cano*, 934 F.3d at 1018-21. The court explained that cell phone searches at the border do not intrude on privacy as greatly as the "highly intrusive investigative techniques" such as "body-cavity searches, x-ray searches, and stomach-pumping," which courts have permitted on the basis of reasonable suspicion rather than a warrant. *Montoya de Hernandez*, 473 U.S. at 551. In all events, the court held that it was constrained to follow binding Second Circuit precedent in *Levy* and *Irving* until the Supreme Court speaks expressly on the issue.

Conclusion

So, where does the law stand? First, some judges may allow limited manual "routine" examination of electronic devices at the border without reasonable suspicion, though the precise scope of that permitted examination is not clear, while other judges would seem to regard all manual searches as "non-routine," and thus may not be conducted without at least reasonable suspicion, and possibly probable cause and a warrant. Second, some judges will allow more intrusive "non-routine" searches of electronic devices at the border based on reasonable suspicion, while other judges would require probable cause and a search warrant.

We can be confident that these issues will be developed further in the Second Circuit, and very possibly in the Supreme Court.

Elkan Abramowitz *and* **Jonathan S. Sack** *are members of Morvillo Abramowitz Grand Iason & Anello. Mr. Abramowitz is a former chief of the criminal division in the U.S. Attorney's Office for the Southern District of New York. Mr. Sack is a former chief of the criminal division in the U.S. Attorney's Office for the Eastern District of New York.* **Emily Smit**, *an associate at the firm, assisted in the preparation of this column.*