Westlaw Today
powered by Reuters

The U.S. is increasingly searching electronic devices at the border

By Andrew Wise, Esq., Richard Gallena, Esq., and Annie Cho, Esq., Miller & Chevalier

APRIL 25, 2024

The U.S. government is more frequently searching individuals' cell phones and other electronic devices at the border under an exception to the Fourth Amendment's general prohibition against warrantless searches.

In 2023, the U.S. Customs and Border Protection (CBP) searched over 41,000 devices,[1] up almost 25% from five years before. Although some courts have started to limit the scope of the border exception, this increasingly common practice poses risks for executives who travel internationally and work for companies in high-risk industries.

There is a federal circuit split demonstrating the dynamic implications of the exception regarding the search of cell phones.

The Fourth Amendment prohibits warrantless searches; however, the Supreme Court has carved out an exception at the U.S. borders, reasoning that such searches are reasonable, "simply by virtue of the fact that they occur at the border."[2] The border search exception was first recognized in *Ramsey* when the Supreme Court held customs officials' warrantless search of incoming envelopes that contained contraband from Thailand was "reasonable."

Courts have since expanded the exception to allow the warrantless search of travelers and their effects (e.g., suitcases, vehicles (including gas tanks), packages) based on the federal government's right to regulate the entry of "unwanted persons and their effects," and a traveler's diminished expectation of privacy at the border.[3]

For years, this has meant that the government's ability to search a traveler's effects has been limited, from a practical perspective, to what a traveler can carry, i.e. luggage. With the rapid advancement of technology and advent of smart phones, however, travelers now carry across the border vast quantities of data about their personal — and professional — life on a regular basis.

Most jurisdictions recognize that the government can search these electronic devices, without a warrant, under the border exception. This can include searches with respect to traditional border-related investigations, but it can also include searches in connection with white collar investigations.

To counter the broad scope of the exception, there have been several legal actions seeking to limit the ability to search cell phones at the border. Unsurprisingly, there is a federal circuit split demonstrating the dynamic implications of the exception regarding the search of cell phones.

A recent 2023 decision in the Southern District of New York, however, suggests a possible shift in the border search exception landscape. Judge Rakoff in *United States v. Smith* held that federal agents must obtain a search warrant upon establishing probable cause to search the contents of one's electric device at the border.[4]

The Court reconciled requiring a warrant with the Supreme Court's decision in *Riley v. California*, which allows law enforcement to search an individual incident to arrest, but requires law enforcement to obtain a warrant before then searching the individual's phone.[5] The Court recognized that an individual's privacy interest in their cell phone differs "fundamentally" from their privacy interest in their bags, and emphasized that the border search exception is not "unlimited," nor is the border "a totally Fourth Amendment-free zone."[6]

The risk that an individual may be stopped and searched is even greater if the individual works for a company that may be under investigation.

Judge Rakoff's decision in *Smith* is the narrowest interpretation of the exception thus far. The Ninth Circuit came close in finding that agents may only conduct warrantless searches of cell phones "only to determine whether the phone contains contraband," like images of child pornography.[7] Agents must establish reasonable suspicion to otherwise conduct a forensic search of a phone.

The Fourth Circuit took a similar, but slightly broader approach from the Ninth Circuit. In *United States v. Kolsuz*, the Fourth Circuit

held that the exception can "accommodate not only the direct interception of contraband as it crosses the border, but also the prevention and disruption of ongoing efforts to export contraband illegally, through searches initiated at the border."[8]

In other words, warrantless searches of cell phones for evidence of illicit activity already underway are deemed reasonable. The Fifth Circuit, however, refused to apply the *Riley* standard and recently held that routine searches of cell phones at the border, "do[] not require either a warrant or reasonable suspicion."[9]

It is unclear whether other courts will follow Judge Rakoff's narrow interpretation of the border search exception. However, some recent decisions suggest a coming paradigm shift in favor of greater protections for travelers at the U.S. border.

Practical guidance

In the meantime, the current application of the border exception leaves individuals — including corporate executives and employees traveling to and from the United States — in a vulnerable position.

The risk that an individual may be stopped and searched is even greater if the individual works for a company that may be under investigation, operates in high-risk industries, or is traveling from certain countries. Indeed, the Chinese government recently alerted[10] Chinese travelers to the risk of being stopped and searched at the U.S. border.

Below we provide practical considerations for individuals and companies:

- Notify your Legal function of when you are traveling, your itinerary, and what company data/devices you are planning to bring.
- If traveling with a company-owned device, consult with the appropriate division within the company to discuss minimizing the volume of company data you carry on your trip. If possible, the company may provide a separate device containing data necessary for the trip.
- It may be best practice to keep your phone turned off upon landing, or turning on "airplane mode," as any copying of the contents will be limited to what is available on the phone. This can help prevent agents from pulling cloud-based data through applications installed on your phone.
- When agents inquire about the nature of your travel, answer truthfully.
- Agents may vaguely attempt to seek your consent or coerce you into unlocking your device. To avoid implicitly consenting, ask the agent to clarify whether they are requesting or ordering you to unlock your device. If a request, you can decline to unlock devices or provide passwords. If an order, then state you are complying under protest.
    - Bear in mind that if you refuse to comply with an order, you may have your device confiscated, your situation may be escalated, or you could be flagged for secondary screening in the future.
- If left alone in the room to unlock your phone or make calls, be aware that you may be monitored.
- Notify the agents if any of your devices contain information that may be protected by the attorney-client privilege.
- Keep record of the names of the agents who searched or confiscated your devices, and request a property receipt for any confiscated items.
- If represented by legal counsel, immediately alert the agents and request to speak with your attorney. Agents may not always agree to the request but make note of it and ensure you inform your counsel immediately after the details of what occurred.

Notes:

[1] https://bit.ly/3Qk71ff

[2] *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

[3] *United States v. Cano*, 934 F.3d 1002, 1013 (citing *United States v. Cotterman*, 709 F.3d 952, 960 (2013)); *see e.g., United States v. Baxter*, 951 F.3d 128, 136 (3d Cir. 2020).

[4] *Smith*, 2023 WL 3358357, at *7, *9 (S.D.N.Y. May 11, 2023).

[5] *Id.*; *Riley*, 573 U.S. 373, 403 (2014).

[6] *Id.* at *5.

[7] *Cano*, 934 F.3d at 1018.

[8] *Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018).

[9] *Malik v. United States Department of Homeland Security*, 78 F.4th 191, 201 (5th Cir. 2023).

[10] https://bit.ly/3QhXwNo

About the authors



Andrew Wise (L), a member at **Miller & Chevalier** and lead of the firm's white-collar defense practice, defends clients in white-collar criminal and civil trials, in addition to representing multinational companies in fraud and anti-corruption investigations. He can be reached at awise@milchev.com. **Richard Gallena** (C), a counsel at the firm, represents companies and individuals in investigations and enforcement actions brought by the U.S. Justice Department, Securities and Exchange Commission and other regulatory authorities. He can be reached at rgallena@milchev.com. **Annie Cho** (R), an associate at the firm, focuses on international anti-corruption, assisting with due diligence, compliance program enhancements and internal investigations. She can be reached at acho@milchev.com All authors are based in Washington, D.C.

This article was first published on Westlaw Today on April 25, 2024.