NACDL FOURTH AMENDMENT CENTER

Device Searches at the Border

A Criminal Defense Lawyer's Primer

April 2025

Protecting digital information at the border remains a critical, uphill battle. CBP **maintains**[1] that it has the broad authority to conduct warrantless (often suspicionless) searches of any digital devices (cellphones, laptops, tablets, etc.) at the border pursuant to the border search exception under the Fourth Amendment.[2] As criminal defense lawyers, NACDL members are highly exposed in this context due to the amount of privileged communications, material and work product present on their devices. The law on this matter is far from settled and currently varies across the country, and as such, requires a case-specific evaluation to determine the level of risk.

What does CBP think it can do?

CBP's last-published official **directive**[3] on electronic device searches was in 2018. It outlines nebulous standards on what border enforcement agents have the power to do. CBP asserts that it can search people crossing the border (this often means ports of entry in airports, but also at land crossings or other ports of entry) without a warrant and without suspicion "to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer."[4] Their 2018 directive outlines the extension of that search authority to digital devices.[5]

The courts refer to most searches of a traveler's person and possessions as a "routine search." CBP agents conducting routine searches do not need a warrant or reasonable suspicion.[6] The guidance and some case law distinguishes between so-called "basic" or "manual" searches and "advanced" or "forensic" searches of digital devices.[7] Manual searches of digital devices require no technical knowledge — they usually involve scrolling through digital files, images, or browser history.[8] These searches are generally conducted on-the-spot during some form of secondary inspection. Forensic searches use external equipment and may involve the assistance of technical experts to probe a device and can result in the detention of the device.[9] By policy, CBP does not require any suspicion to conduct a basic search but does require reasonable suspicion for advanced searches.[10]

CBP's policy further states that officers can only search information stored locally on a device (not in the cloud), and should make sure a device is in airplane mode before searching it.[11] As part of a border search, CBP allows officers to detain devices or copies of their information ostensibly for up to five days, which may include sending it to an off-site location.[12] However, there is no actual threshold for how long a device can be held as CBP allows itself to extend the five-day rule essentially indefinitely and for undefined reasons. The information must then be destroyed unless there is probable cause.[13] CBP's policy is unclear as to what justification is required for detaining a device or what procedures there are for ensuring that the information is properly destroyed, and people's devices have, in some cases, been held for weeks or months.

CBP policy further allows sharing all or portions of device information with other federal enforcement agencies (such as ICE and HSI), at which point, that information will be governed by the policies of that agency.[14] It is unclear what justifies sharing the information with other agencies or what protocols are in place to protect information across agency communication.

Regarding attorneys, CBP's directive contains a section with procedures for "information [officers] identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine:"

"5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

"5.2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office. In coordination with the CBP Associate/Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, **Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission.** (emphasis added) This segregation process will occur through the establishment and employment of a Filter Team composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/Assistant Chief Counsel office.

"5.2.1.3 At the completion of the CBP review, **unless any materials are identified that indicate an imminent threat to homeland security** (emphasis added), copies of materials maintained by CBP and determined to be privileged will be destroyed, except for any copy maintained in coordination with the CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.

. . .

"5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with agencies or entities that have mechanisms in place to protect appropriately such information, and such information will only be shared in accordance with this Directive."[15]

It is critical to understand that the above creates no real standard. It provides the appearance of a "protocol" regarding privileged information but does not actually create any enforceable protocol, procedure, or rules. It allows officers to essentially behave without any rules per their own judgment. No particular level of suspicion or judicial approval is required to search privileged information. There are no definitions or explanations as to what CBP considers "appropriate measures" or "appropriate" handling of this information. There are no guidelines as to when privileged information will be shared with agencies or what other agencies should do to "protect appropriately" such information.

Moreover, the requirement that the individual being searched has to first identify the privileged information themselves is highly problematic. Not only does this specifically alert CBP officers to the most sensitive data, but it is also incredibly difficult for an attorney to identify anything that might be "privileged" among years of emails, documents, and communications likely accessible from their device in an on-the-spot manner in an interrogation room. Identifying privileged information normally takes teams of people and extended time going through each item.

Legal Landscape

The Supreme Court has not addressed the border search exception's application to electronic devices. However, appellate courts have created some **limits**[16] on its application to devices, and more recently, some notable district court rulings have found that a warrant is required to search cell phones at the border. Many civil liberties organizations, including the ACLU and EFF, petitioned the Supreme Court to address the issue in 2021 and the petition was **denied**.[17] In that case, ***Merchant v Mayorkas* (2021)**,[18] the Court was asked to consider whether a warrant is required to search electronic devices at the border **after**[19] a district court ruling requiring reasonable suspicion for such a search and a First Circuit Court of Appeals reversal. The plaintiffs were all U.S. citizens or lawful permanent residents who had devices searched upon reentering the country and several of them had devices seized for weeks or months.

In ***Riley v. California* (2014)**,[20] the Supreme Court held that a warrant is required to search a cell phone seized from someone who has been arrested. In other words, the Court found that a "search incident to arrest" does not apply to data on cell phones. This ruling

provided the basis for a few subsequent circuit court opinions on the subject imposing some limitations on border device searches. An older Supreme Court case, ***United States v. Montoya de Hernandez* (1985)**,[21] is often cited in decisions on device searches for the proposition that the border search exception requires balancing the government's interests with the Fourth Amendment rights of the person being searched.

At the appellate level, in ***United States v. Cano* (9th Cir. 2019)**,[22] the court held that forensic searches of devices are only permissible when officers have reasonable suspicion that the device contains digital contraband, and that any search — whether manual or forensic — must be limited in scope to searching for digital contraband. In this case, the defendant was referred to secondary inspection and found to be carrying cocaine in his car tire. While in custody, his cell phone was searched both manually and forensically. These searches included examining his messages, call logs, etc., and the court found that the warrantless search of data *not limited to searching for digital contraband* exceeded the scope of the border search exception. Similarly, ***United States v. Aigbekaen* (4th Cir. 2019)**,[23] held that a forensic device search requires a warrant when officers are conducting the search to advance a pre-existing investigation of domestic crime. The defendant in *Aigbekaen* was being investigated for sex trafficking, and the devices were searched forensically without a warrant upon entry to the United States. The court found that these searches lacked appropriate nexus to a border search because the investigation was for purely "domestic" crimes. Notably, the Eleventh Circuit has held directly opposite to the aforementioned. In ***United States v. Touset***,[24] the court evaluated a device search pursuant to a child pornography investigation and found that no reasonable suspicion is required for electronic device searches at the border because this would create "special protection for the property most often used to store and disseminate child pornography." *Id.* at 16.

However, some promising recent district court decisions have gone even further than the Ninth and Fourth Circuits and signaled some willingness to further limit or ban warrantless digital searches at the border altogether. However, none of these cases have yet been addressed by higher courts. Most courts considering the issue have distinguished between manual and forensic searches, with forensic searches seemingly subject to higher scrutiny based on the seizure of the device, the circumstances surrounding the seizure or a delayed search, and the invasive nature of copying all the contents of a device. Of note is that many of these cases also contain facts regarding compelled decryption (people being forced to give up their passcode or unlock their device). Please refer to our materials on **compelled decryption**[25] for further analysis on this.

Recent Cases

***U.S. v. Fox* (E.D.N.Y. July 2024)**[26]

HSI created a travel notification for the accused pursuant to an investigation for fraud and money laundering. The agent involved waited for defendant to enter the United States after travel and then seized her devices, which were sent out-of-state for a forensic search. The EDNY found that reasonable suspicion of criminal activity would be required at the border to search defendant's cell phone, and that the border-search exception did not apply in this instance, requiring a warrant for the search. Further, the court found that the good-faith exception did not apply.

***U.S. v. Sultanov* (E.D.N.Y. July 2024)**[27]

The accused was detained in secondary inspection at JFK pursuant to an investigation regarding possession of child sexual abuse material and his device was manually searched (and he was directed to provide his passcode). Based on the information from the warrantless manual search, agents then obtained a warrant to forensically search the accused's other devices. The EDNY found that the border search exception does not apply to cell phones and that manual and forensic searches constitute an equal invasion of privacy. The court held that the Fourth Amendment generally requires a warrant based on probable cause to search a cell phone at the border.

***U.S. v. Smith* (S.D.N.Y. March 2023)**[28]

The accused was detained at Newark airport and compelled to provide his cell phone passcode. The device was searched manually and an electronic copy of the contents was also created without a warrant. A warrant was subsequently sought several weeks later. This SDNY ruling was significant in applying the reasoning of ***Riley v. California* (2014)**[29] squarely to the issue of cell phones and finding that a warrant was generally required to search and copy a U.S. citizen's cell phone at the border. The court stated that "[n]one of the rationales supporting the border search exception [justify] applying it to searches of digital information contained on a traveler's cell phone, and the magnitude of the privacy invasion caused by such searches dwarfs that historically posed by border searches." This case has been **appealed**[30] to the 2nd Circuit. Another case on this subject, ***U.S. v. Kamaldoss* (E.D.N.Y. April 2022)**,[31] in which the

warrantless forensic search was upheld by the district court, has also been **appealed**[32] to the 2nd Circuit.

***U.S. v. Djibo* (E.D.N.Y. December 2015)**[33]

The accused's identity and contact information were identified via the warrantless device search of another traveler found in possession of heroin. As a result, officials created a travel alert for defendant, and he was searched and detained by CBP at JFK prior to an outbound flight, during which he was directed to provide passcodes, and his devices were searched. The court held that the warrantless forensic search via Cellebrite of defendant's device was unconstitutional and further search of the cell phone pursuant to a warrant was the fruit of the poisonous tree due to the illegal initial search.

What are your rights at the border?

In short, it varies based on citizenship status. In general, attempting to refuse a search can **risk**[34] detention and seizure of your devices. However, if you are a U.S. Citizen, you must be allowed to enter the country. Lawful permanent residents now face uncertain immigration **risks**[35] in general, and it is unclear what consequences may occur regarding device searches. Non-citizens refusing a device search risk detention, denial of entry, and deportation.

Best Practices for Attorneys

1. In general, try to carry as little digital information and the minimal number of devices possible.
2. Specific devices can be used as travel-only to limit the amount of content accessible, with all sensitive data encrypted or password-protected.
3. Use strong alphanumeric passwords to access the device instead of biometric access (face ID or thumbprint).
4. Store data on the cloud as opposed to locally on the device. This may depend on what is available on your specific device as sometimes data is stored both on the cloud and locally.
5. Keep devices shut down or on airplane mode while crossing the border.
6. Someone being searched or detained by CBP will not be able to communicate with the outside world. One option to ensure some degree of protection for traveling attorneys is to arrange a "buddy system": arrange for another lawyer to appear at a port of entry if the traveling attorney does not make contact within a given time span after arrival. The second lawyer can act as a monitor in case the traveler is detained.
7. The Second Circuit case ***U.S. v. Kovel* (2d Cir. 1961)**[36] held that confidential communications between a client and an accountant hired by a law firm specifically for the purpose of legal advice covered by the attorney-client privilege. Practitioners of tax law often use so-called *Kovel* letters to ensure that outside experts can engage in privileged communications, though under a number of specific limitations. *Kovel* letters might be used to ensure that investigators traveling overseas can assert attorney-client privilege at the border.
8. A court may grant a protective order under Rule 16(d) of the Federal Rules of Criminal Procedure. The potential for the violation of attorney-client privilege or work-product privilege at the border may constitute good cause for a judge to issue a protective order for a digital device.
9. Attorneys who are traveling may benefit from a small card printed with the text of Rule 1.6 of the Model Rules of Professional Conduct (Confidentiality) to show to CBP agents.

Further Resources

- Esha Bhandari, Nathan Freed Wessler, and Noa Yachot, "Can Border Agents Search Your Electronic Devices? It's Complicated," ACLU of Texas (March 21, 2025), (**https://www.aclutx.org/en/news/can-border-agents-search-your-electronic-devices-its-complicated**)
- Sophia Cope, Amul Kalia, Seth Schoen, and Adam Schwartz, "Digital Privacy at the U.S. Border: Protecting the Data On Your Devices," Electronic Frontier Foundation (December 2017), (**https://www.eff.org/wp/digital-privacy-us-border-2017**)
- Sophia Cope, "Federal Judge Makes History in Holding That Border Searches of Cell Phones Require a Warrant," Electronic Frontier Foundation (May 30, 2023), (**https://www.eff.org/deeplinks/2023/05/federal-judge-makes-history-holding-border-searches-cell-phones-require-warrant**)
- Johana Bhuiyan, "How to protect your phone and data privacy at the US border," The Guardian (March 26, 2025), (**https://www.theguardian.com/technology/2025/mar/26/phone-search-privacy-us-border-immigration**)
- Gaby Del Valle, "Is it safe to travel with your phone right now?", The Verge (March 23, 2025), (**https://www.theverge.com/policy/634264/customs-border-protection-search-phone-airport-rights**) Andy Greenberg, Matt Burgess, "How to Enter the US With Your Digital Privacy Intact," Wired (March 24, 2025), (**https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact/**)

Endnotes

1. *See* U.S. Customs and Border Protection Website, "Search Authority — Border Search of Electronic Devices at Ports of Entry," (**https://www.cbp.gov/travel/cbp-search-authority/border-search-electronic-devices**).
2. The border search exception holds that the government's interest in determining the admissibility of goods and people at the border generally outweighs any individual traveler's privacy rights against warrantless search. *See* Sophia Cope et al., *Digital Privacy and the U.S. Border: Protecting the Data on Your Devices and the Cloud*, Electronic Frontier Foundation (2017), at 24 n. 24 (collecting Supreme Court cases).
3. *See* U.S. Customs and Border Protection, CBP Directive 3340-049A (Jan. 4, 2018) at 3 (Describing the statutory authority for border searches, "[*s*]*ee*, e.g., 8 U.S.C. §§ 1225, 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a; *see also* 19 C.F.R. § 162.6 ('All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer.')," (**https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf**).
4. *Id.*
5. U.S. Customs and Border Protection, *supra* note 1; U.S. Immigration and Customs Enforcement, ICE Directive No. 7-6.1 (Aug. 18, 2009); Plaintiffs' Mot. for Summary Judgment Ex. 20, *Alasaad v. Nielsen*, 419 F. Supp. 3d 142 (D. Mass. 2019) (HSI legal update issued in response to litigation).
6. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant…").
7. CBP's updated directive and ICE's legal update introduce a shared definition of advanced searches. *See, e.g.,* U.S. Customs and Border Protection, *supra* note 1 at 5 ("An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."). *But see Alasaad v. Nielsen*, 419 F.Supp.3d 142, 165 (D. Mass. Nov. 12, 2019) ("the Court is unable to discern a meaningful difference between the two classes of searches in terms of the privacy interests implicated.").
8. *See, e.g., Abidor v. Napolitano*, 990 F.Supp.2d 260, 260-270 (E.D. N.Y. 2013) ("A quick look entails only a cursory search that an officer may perform manually. It involves opening the computer and viewing the computer's contents as any lay person might be capable of doing simply by clicking through various folders."); *Alasaad, supra* note 3 at 163 ("[I]n a basic search, agents can peruse and search the contents of the device, using the native search functions on the device, including, if available, a keyword search.").
9. *See, e.g., United States v. Kolsuz*, 890 F.3d 133, 139 (4th Cir. 2018) (border search case where phone was transported four miles to HSI office, where it was held for a month while a "Computer Forensic Agent . . . attached the phone to a Cellebrite Physical Analyzer, which extracts data from electronic devices, and conducted an advanced logical file system extraction.").
10. CBP specifies that this suspicion must be of "activity in violation of the laws enforced or administered by CBP," unless there is a "national security concern." U.S. Customs and Border Protection, *supra* note 1 at 5. It is unclear if ICE has the same national security exception. *See Alasaad*, *supra* note 3 at 149 n.2.
11. U.S. Customs and Border Protection, *supra* note 1 at 4.
12. U.S. Customs and Border Protection, *supra* note 1 at 7.
13. *Id*. at 7, 9, 10. CBP specifies that the probable cause must be that the device "contains evidence of a violation of law that CBP is authorized to enforce or administer." *Id*. at 9. Without probable cause, CBP can retain information "relating to immigration, customs, and other enforcement matters" in relevant databases. *Id*. at 9-10. Sharing is allowed "to the extent consistent with applicable law and policy." *Id.* at 10.
14. Id. at 10.
15. U.S. Customs and Border Protection, *supra* note 1 at 5-6.
16. *See* Sophia Cope, *Federal Judge Makes History in Holding That Border Searches of Cell Phones Require a Warrant*, Electronic Frontier Foundation (2023), (**https://www.eff.org/deeplinks/2023/05/federal-judge-makes-history-holding-border-searches-cell-phones-require-warrant**).
17. *See* SCOTUSblog, *Merchant v. Mayorkas* (2021), **https://www.scotusblog.com/case-files/cases/merchant-v-mayorkas/**.

18. *See* Electronic Frontier Foundation, *Merchant v. Mayorkas*-petition for writ of certiorari (2021), **https://www.eff.org/document/merchant-v-mayorkas-petition-writ-certiorari**.
19. *See* ACLU, *Merchant v. Mayorkas* (2021) case page, **https://www.aclu.org/cases/merchant-v-mayorkas**.
20. *Riley v. California,* 573 U.S. 373 (2014), **https://supreme.justia.com/cases/federal/us/573/373/**.
21. *United States v. Montoya de Hernandez,* 473 U.S. 531 (1985), **https://supreme.justia.com/cases/federal/us/473/531/**.
22. *United States v. Cano,* 934 F.3d 1002 (2019), **https://law.justia.com/cases/federal/appellate-courts/ca9/17-50151/17-50151-2019-08-16.html**.
23. *United States v. Aigbekaen,* Case No. 17-4109 (4th Cir. 2019), **https://law.justia.com/cases/federal/appellate-courts/ca4/17-4109/17-4109-2019-11-21.html**.
24. *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018), **https://law.justia.com/cases/federal/appellate-courts/ca11/17-11561/17-11561-2018-05-23.html**.
25. *See* NACDL, *Compelled Decryption Primer* (2019), https://www.nacdl.org/nacdl/media/image_library/Elements/Advertisements/CompelledDecryptionPrimer_1.pdf .
26. *United States v. Fox*, Case No. 23-CR-227 (NGG) (E.D.N.Y. July 24, 2024), **https://scholar.google.com/scholar_case?case=8772180833477562892**.
27. *United States v. Sultanov,* Case No. 22-CR-149 (NRM) (E.D.N.Y. July 24, 2024), **https://scholar.google.com/scholar_case?case=10750649489421943627**.
28. *United States v. Smith*, Case No. 22-CR-352 (JSR) (S.D.N.Y. March 17, 2023), **https://s3.documentcloud.org/documents/23813619/us-v-smith.pdf**.
29. *Riley v. California,* 573 U.S. 373 (2014).
30. *See* Sophia Cope, *EFF Tells the Second Circuit a Second Time That Electronic Device Searches at the Border Require a Warrant,* Electronic Frontier Foundation (Nov. 26, 2024), **https://www.eff.org/deeplinks/2024/11/eff-tells-second-circuit-second-time-electronic-device-searches-border-require**.
31. *United States v. Kamaldoss*, Case No. 19-CR-543 (ARR) (E.D.N.Y. April 22, 2022), **https://scholar.google.com/scholar_case?case=7162125519521470905**.
32. *See* Sophia Cope, *EFF to Second. Circuit: Electronic Device Searches at the Border Require a Warrant,* Electronic Frontier Foundation (Nov. 8, 2024), **https://www.eff.org/deeplinks/2024/11/eff-second-circuit-electronic-device-searches-border-require-warrant**.
33. *United States v. Djibo,* 151 F. Supp. 3d 297 (E.D.N.Y. Dec. 16, 2015), **https://www.courtlistener.com/opinion/7317407/united-states-v-djibo/pdf/**.
34. *See* Mithil Aggarwal, *Denied, deported, detained: U.S. border incidents have travelers thinking twice,* NBC News (March 29, 2025), **https://www.nbcnews.com/news/world/trump-immigration-detained-visitors-border-search-device-visa-passport-rcna197736**.
35. *See* Juliana Kim, *What green-card and visa holders should know before traveling abroad*, NPR (March 25, 2025), **https://www.npr.org/2025/03/29/nx-s1-5343493/green-card-holders-rights-visa-detained-cbp**.
36. *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).

About the National Association of Criminal Defense Lawyers (NACDL)

The National Association of Criminal Defense Lawyers (NACDL) envisions a society where all individuals receive fair, rational, and humane treatment within the criminal legal system.

NACDL's mission is to serve as a leader, alongside diverse coalitions, in identifying and reforming flaws and inequities in the criminal legal system, and redressing systemic racism, and ensuring that its members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level.

About the Fourth Amendment Center

NACDL's Fourth Amendment Center offers direct assistance to defense lawyers handling cases involving new surveillance tools, technologies and tactics that infringe on the constitutional rights of people in America.

The Center is available to help members of the defense bar in bringing new Fourth Amendment challenges. To request assistance or additional information, contact **4AC@nacdl.org**.

About the NACDL Foundation for Criminal Justice (NFCJ)

NACDL's Fourth Amendment Center is supported by contributions made to the NACDL Foundation for Criminal Justice (NFCJ), a 501(c)(3) charity. The mission of the NFCJ is to preserve and promote the core values of America's justice system guaranteed by the Constitution — among them due process, freedom from unreasonable search and seizure, fair sentencing and effective assistance of counsel — by educating the public and the legal profession to the role of these rights and values in a free society.

How to Support Our Work

You can support our mission and enhance your career by becoming a member of the NACDL or by making a tax-deductible donation to the NFCJ. Learn more by visiting **NACDL.org/Landing/JoinNow** or **NFCJ.org/support**.

NACDL FOURTH
AMENDMENT CENTER

For litigation assistance and other resources contact 4AC@nacdl.org