SEARCHES OF ELECTRONIC DEVICES AT PORTS OF ENTRY

Kyle Sweetland, Amy Peikoff, and Mitchell Scacchi

Customs and Border Protection (CBP) officers may prevent the entry of people or property at the US border and at ports of entry. Increasingly, CBP officers also perform warrantless searches of personal electronic devices such as cell phones and computers. CBP officers sometimes even retain data from devices. The stated purpose for these activities is to stop harmful content, terrorists, and illegal immigrants from entering the United States,[1] but legal experts argue that these practices violate the Fourth Amendment's prohibition of unreasonable searches and seizures.[2]

In the past decade, the number of electronic device searches at ports of entry more than quadrupled, from around 8,500 in 2015 to over 46,000 in 2024 (see Figure 1). That trend continues apace in 2025, with the third fiscal quarter showing CBP having searched 14,899 people—the highest number on record and 16.7 percent higher than the next-highest quarterly figure of 12,766 set in the second fiscal quarter of 2022.[3]

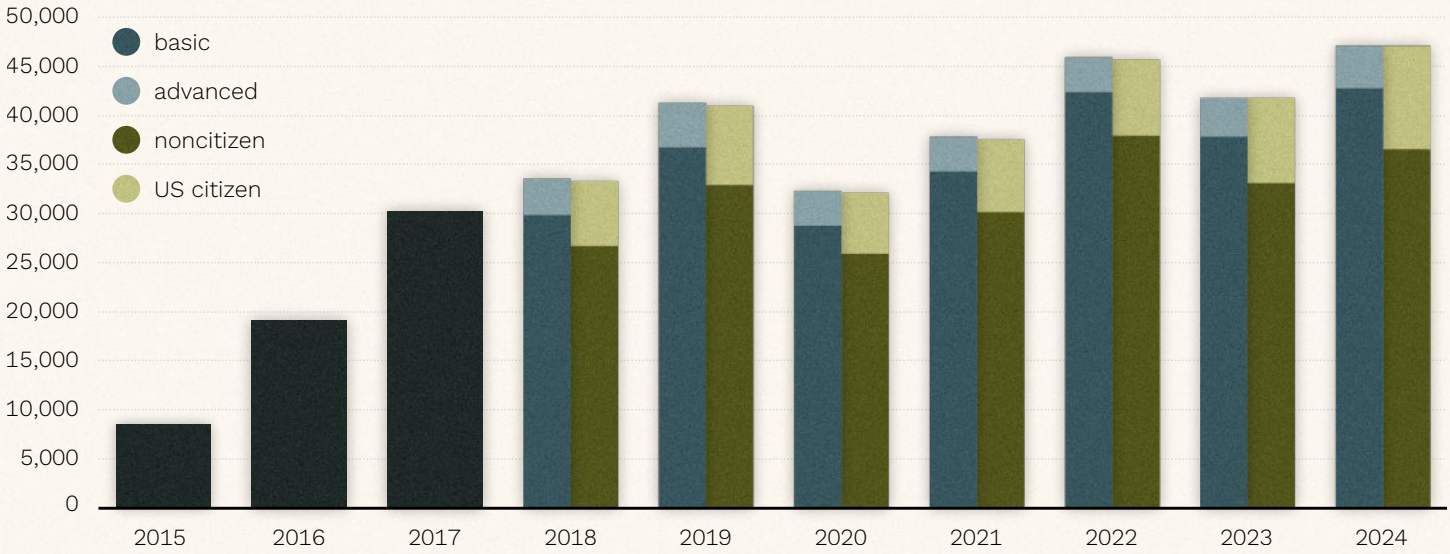
A basic search involves visually inspecting a device and scrolling through its contents. An advanced search uses external equipment to review, copy, and retain device contents for later analysis.[4] From 2018 to 2024, most searches of electronic devices at ports of entry were basic searches of non-citizens' devices, as Figure 1 shows. Nonetheless, about 10 percent of all searches were advanced searches, and about 20 percent of all searched devices belonged to US citizens.

Searches can result in arrest if criminal activity is found.[5] Non-citizens have been detained and denied entry to the country as a result of searches.[6] US citizens will not be prevented from entering the country or arrested for refusing to provide officers with their device's password, though they may not be timely or correctly informed of these or other rights they have at the beginning of the search process.[7]

People who refuse the search process are subject to interrogation and seizure of their electronic device or the contents on it, even if those contents are protected from access by federal law.[8] The default holding period for devices and data is five days, but this timeframe can be extended by seven-day increments,[9] with some people reporting their devices being held for weeks or months.[10]

Officers can review and keep data stored on the device itself only if it is related to immigration, customs, and other CBP enforcement matters or if it contains evidence of a violation of a CBP-enforced law.[11] Once obtained, this data can be shared with other agencies and is stored in a computerized system called the Automated Targeting System (ATS) for up to 15 years—or longer in special circumstances.[12] This electronic device data is combined with other data in ATS to create a risk profile and help officers identify persons—also known as "lookouts"—who are deemed to warrant secondary inspection when crossing the border in the future.[13]

FIGURE 1. ELECTRONIC DEVICE SEARCHES BY TYPE AND BY CITIZENSHIP STATUS (FY 2015–2024)



Note: Data were not broken down by search type and citizenship status until fiscal year (FY) 2018 under 2018 CBP Directive 3340-049A.
Sources: FY 2015: Customs and Border Protection, "CBP Releases Statistics on Electronic Device Searches," news release, April 11, 2017, https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0; FY 2016–2017: Customs and Border Protection, "CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics," news release, January 5, 2018, https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and; FY 2018–2022: CBP FOIA request, available upon request; FY 2023–2024: "CBP Enforcement Statistics Fiscal Year 2024," Customs and Border Protection, last modified November 19, 2024, https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics-fy2024.

NOTES

1. Customs and Border Protection, "Border Search of Electronic Devices at Ports of Entry," last updated August 13, 2025, https://www.cbp.gov/travel/cbp-search-authority/border-search-electronic-devices.

2. Esha Bhandari, Nathan Freed Wessler, and Noa Yachot, "Can Border Agents Search Your Electronic Devices? It's Complicated," American Civil Liberties Union of Texas, last updated March 21, 2025; Brief for Reporters Committee for Freedom of the Press as Amici Curiae Supporting Defendant, United States v. Alisigwe No. 24-960 (2d Cir. 2024); Brief for Electronic Privacy Information Center as Amici Curiae Supporting Plaintiff, Anibowei v. Wolf, 70 F.4th 898 (5th Cir. 2023) (No. 20-10059).

3. Matt Burgess, "Phone Searches at the US Border Hit a Record High," *WIRED*, August 20, 2025.

4. "Border Search of Electronic Devices at Ports of Entry."

5. Hillel R. Smith, "U.S. Customs and Border Protection's Powers and Limitations: A Primer" (CRS report no. LSB10559, Congressional Research Service, Washington, DC, November 30, 2021).

6. Mithil Aggarwal, "Denied, Deported, Detained: U.S. Border Incidents Have Travelers Thinking Twice," *NBC News*, March 29, 2025.

7. Ron Wyden to Chris Magnus, September 15, 2022, letter to CBP on border searches of devices.

8. Caitlynn Peetz Stephens, "A Superintendent Was Held 5 Hours by Border Agents. What Was His Top Concern?," *Education Week*, July 30, 2025.

9. Customs and Border Protection, "Border Searches of Electronic Devices" (CBP Directive no. 3340-049A, Customs and Border Protection, Washington, DC, January 4, 2018), 7, sections 5.4.1 and 5.4.1.1.

10. Bhandari, Freed Wessler, and Yachot, "Can Border Agents Search?"

11. Dana Khabbaz, "How CBP Uses Hacking Technology to Search International Travelers' Phones," *Electronic Privacy Information Center*, February 22, 2022; "Border Search of Electronic Devices at Ports of Entry."

12. "Border Search of Electronic Devices at Ports of Entry"; Statement of Undisputed Material Facts in Support of Pls.' Mot. for Summ. J., Alasaad v. Nielsen, No. 1:17-cv-11730-DJC (D. Mass. Apr. 30, 2019).

13. US Department of Homeland Security, *Privacy Impact Assessment for the Automated Targeting System DHS/CBP/PIA-006(b)*, June 1, 2012; Statement of Undisputed Material Facts.