Foster Garvey

Legal Alerts

Border Searches of Personal Electronic Devices: What International Travelers Should Know

08.18.25 04.30.26

With evolving enforcement priorities and heightened scrutiny at ports of entry, travelers arriving in or departing from the United States may encounter increased inspections of personal electronic devices by U.S. Customs and Border Protection (CBP). These inspections may be triggered by a range of factors, including irregularities with travel documents or visas, past immigration or criminal violations, security watchlists or entirely at random.

CBP officers are granted broad authority under federal law to search electronic devices at the border. This authority applies during both primary inspection and any secondary screening or temporary detention. Officers may conduct a basic search, such as reviewing content stored directly on the device, or, in some cases, an advanced search, which involves connecting the device to external systems to review, copy and analyze its contents more thoroughly.

Importantly, CBP's authority is limited to data stored locally on the device. In general, officers are instructed not to access information stored remotely, such as files accessed via cloud-based services, messaging platforms or mobile networks. To avoid accessing remote content inadvertently, travelers may decide to disable Wi-Fi, Bluetooth and cellular connections before an inspection. On the other hand, CBP officers may also take steps to ensure network access is disabled when necessary, particularly in cases involving national security or criminal investigations.

Travelers may be asked to provide device passcodes or biometric access to unlock their phones, tablets or laptops. CBP policy states that passcodes must be used only to facilitate the search and are to be deleted or destroyed after the inspection. While travelers are not legally required to provide passcodes, refusal may result in temporary seizure of the device or extended detention.

Devices containing sensitive or protected material, such as attorney-client privileged communications, medical or financial records, trade secrets or journalistic work product, are subject to additional legal safeguards. CBP officers are required to follow internal procedures and applicable federal laws when handling privileged or confidential data, including pausing a search and consulting CBP counsel if privilege is asserted.

As border search policies remain active and continue to develop, individuals and businesses should consider precautions when traveling internationally. This may include traveling with minimal data, using temporary or encrypted devices or ensuring confidential content is not stored locally.

For questions about how to reduce risk or safeguard personal or business information during international travel, please contact our Immigration team.

Authored by

Leo C. Peng

Principal|Seattle

206.816.1537 leo.peng@foster.com

Related Areas

- Immigration