AMERICAN ASSOCIATION OF UNIVERSITY PROFESSORS

1133 19th Street, NW, Suite 200, Washington, DC 20036
Phone: 202.737.5900 • **Fax:** 202.737.5526 • **www.aaup.org**

July 31, 2017

FAQs on Border Inspection

NOTE: The following general information is not a substitute for legal advice. You should consult an attorney if you have specific legal questions about your particular situation.

1. Do I have the same legal rights at the border that I would elsewhere in the United States?

No, because of the so-called "border search exception." The Fourth Amendment to the US Constitution generally forbids "unreasonable searches and seizures" by the government. However, the Supreme Court has held that at the border (which includes international ports of entry like airports), the government has broad authority "pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." That heightened governmental interest in security, combined with a lower expectation of privacy at the border than in the interior, has led the Supreme Court to conclude that "routine" border searches are "not subject to any requirement of reasonable suspicion, probable cause, or warrant." However, a class of "non-routine" border searches require at least some level of particularized suspicion, if they are particularly intrusive, destructive, or offensive.

Although the Supreme Court has not addressed specifically the search of electronic devices at the border, other federal courts generally agree that such searches do not require even reasonable suspicion—consistent with the general rule. One exception is the US Court of Appeals for the Ninth Circuit (covering Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, and Washington), which held in 2013 that reasonable suspicion must underlie the "forensic examination" of a computer hard drive taken at the border.

Given this legal landscape, US Customs and Border Protection (CBP) claims broad authority to search and seize electronic devices at the border, and has issued Directive No. 3340-049 on the Border Search of Electronic Devices Containing Information (hereafter referred to as the "Directive").

2. Didn't the Supreme Court rule that the police must get a warrant before searching someone's cell phone?

Yes, but that case did not involve a border search. In *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court held that a warrant is generally required before a search of a cell phone seized incident to arrest. While there is an argument that similar reasoning could be applied to border searches, so far, lower courts have typically declined to extend *Riley* to limit border searches of electronic devices.

3. So could my laptop, phone, or other electronic device be searched if I am a US citizen returning from traveling abroad?

Yes, even if you are a US citizen or a lawful permanent resident (LPR, or "green card" holder). According to the CBP (https://www.cbp.gov/sites/default/files/documents/inspection- electronic-devices-tearsheet.pdf), a

traveler may be chosen for inspection for many different reasons (for example, randomly, or because his or her name matches a "person of interest" in the government's databases, or because his or her travel documents are incomplete). As DHS itself has emphasized, the Equal Protection Clause forbids intentional discrimination by the federal government on account of race, religion, or ethnicity, and thus these should not serve as a reason or factor for conducting discretionary border searches.

4. What about the data on my phone, computer, or other electronic device?

The Directive allows CBP officers and border agents to search travelers' electronic devices, including "any device that may contain information, such as computers . . . mobile phones . . . and any other electronic or digital devices," CBP agents may swipe through your phone or look through the documents on your computer. The government also claims the authority to copy the data on your electronic devices. After the information on the devices has been reviewed, if no probable cause exists to seize that information, any copies of the information must be destroyed and the devices must be returned, ordinarily within seven days of the determination of no probable cause

Under the Directive, CBP officers may share copies of information contained in electronic devices "with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy." And the Directive provides that CBP officers "will promptly share any terrorism information encountered in the course of a border search with elements of the federal government responsible for analyzing terrorist threat information."

5. Can CBP agents ask for my thumbprint or passcode/PIN to unlock my electronic device, or for my email or social media passwords?

Yes, even if you are a US citizen or a lawful permanent resident (LPR, or "green card" holder). The law on whether you are legally required to comply is unsettled.

Regarding the information required to unlock your electronic device, it has been reported that CBP takes the position that it has the right to obtain and keep passwords as necessary to facilitate digital searches of a device that has been detained.

Regarding email and social media, some privacy experts contend that the "border search exception" would not apply to a CBP search of online accounts because the data is hosted at data centers around the world, not on the device carried through the border. However, this legal issue has not been settled, and as a practical matter, once CBP gains access to your device, CBP will have access to your signed-in online applications (Facebook, Twitter, etc.).

6. What if I refuse to provide my PIN or passwords?

If you are a US citizen, you cannot legally be denied entry into the United States, but you may be detained and delayed, and there is a chance your phone, laptop, or other electronic device will be seized. If you are a lawful permanent resident (LPR, or "green card" holder), in addition to the complications that a US citizen may face, a hearing before an immigration judge might be required. If you are a foreign national (for example, a visa

holder), and you are perceived as failing to cooperate, CBP might deny you entry.

7. Might the government keep my phone, computer, or other electronic device?

The Directive authorizes the detention of electronic devices, or information copied from them, for "a brief, reasonable period of time to perform a thorough border search," whether conducted on- or off-site. Absent "extenuating circumstances," the detention of devices "ordinarily should not exceed five (5) days."

8. What should I do if CBP asks to search my phone, laptop, or other electronic device, or for my passwords?

CBP has the legal authority to perform a routine search of electronic devices that you carry across the border. If CBP decides to question you, or inspect your electronic device(s), you should never lie to or attempt to deceive CBP personnel, or try to obstruct the investigation (for example, by deleting data). CBP personnel are federal agents, and lying to federal agents or knowingly interfering with their investigation is a crime.

Each individual should assess the risks and rewards of refusing a request from a CBP or ICE official. For Foreign Nationals entering the United States, non-compliance can be grounds for the denial of entry and deportation. For US citizens or legal residents, it may result in detainment of your device and/or costly delays to you (for example, missed flights). If you have material on your device that you feel is sensitive or proprietary, it is recommended that you tell the CBP/ICE agent this and ask that they take this into consideration when conducting their search.

In conjunction with the Knight First Amendment Institute at Columbia University, the AAUP is seeking information from any faculty members who have had their cell phones or other electronic devices searched by US border patrol officers at the nation's borders while traveling internationally. If you have been subject to such a search please send an email with a brief description of your experience if possible and your contact information to katie.fallow@knightcolumbia.org. Your information will remain confidential.

9. What should I do to protect my data when traveling abroad?

If you do not want a particular electronic device searched, do not travel internationally with it. You should be wary about including on a laptop that you take overseas any financial or other personal information that you would not want viewed without your permission. If you need to travel internationally with electronic devices, the safest course is to travel with devices that contain only the specific files needed for the trip. If your device contains controlled software or sensitive data—particularly data that may be controlled under federal or state law or regulations—it is recommended that you do not travel with it, especially internationally. If a device is to be used only for making presentations, consider taking a memory stick or storing the presentation on a cloud-based server instead. If you are using a device for other purposes (such as email), consider taking a "clean" computer that does not include the restricted software, data, or other sensitive information.

10. Is the inspection of your IT device part of a new policy or law that Customs and Border Patrol (CBP) and Immigration and Customs Enforcement (ICE) agents enforce?

No, the ability of Immigration and Customs officials to search your personal belongings when crossing a border in order to ensure that no violation of US law has occurred is one of the key purposes of having inspections at the points of entry and exit. With the increase in everyday use of technology by average citizens, the expansion of searches into technological devices traveling with them occurred years ago. In 2013, a DHS assessment of the practice claimed that the "clear and longstanding" authority "to conduct border searches without suspicion or warrant" extends to searches of electronic devices, and that imposing a reasonable suspicion requirement on such searches "would be operationally harmful without concomitant civil rights/civil liberties benefits." DHS therefore concluded that the Directive does not violate the Fourth Amendment, and it rejected calls to adopt a reasonable suspicion standard as a policy choice.

11. How often do searches of electronic devices occur?

While the topic has hit social media venues quite a bit in early 2017 given a few high profile incidents, according to the *New York Times*, the number of searches has been relatively low. In the article, a US Customs agency spokesman quoted said that only "4,444 cellular phones and 320 other electronic devices were inspected in 2015 which represented 0.0012 percent of the 383 million arrivals that year." However, the article went on to suggest that there may have been significantly higher numbers in 2016. (https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html?_r=0)

12. What do I do if they detain my device?

If your device is detained, you will be given a receipt for it. Do not leave the airport without first having this documentation. Further, it is recommended that you copy or take a photo of the serial numbers from each device that you'll be traveling with and leave a copy/photo with a colleague or family member at home. This is also recommended for travelers in general as the serial numbers are helpful if a device is stolen while a traveler is abroad. Serial numbers help in the identification of the device and tracking in the event that a device is stolen or lost during detainment.

13. What should I do if a non-US (host country) border agent asks to inspect my device or requests my password/login credentials?

As often happens in the immigration space, travelers may see reciprocal treatment when they reach the non-US destinations. Careful consideration should be given to what the risks are should you chose not to comply. A follow-up report to the nearest US embassy or consulate is recommended. (If you are not a US citizen, report the detainment to the embassy or consulate of your nation.)