Digital Privacy at the U.S. Border

PROTECTING THE DATA ON YOUR DEVICES AND IN THE CLOUD

Sophia Cope, Staff Attorney

Amul Kalia, Analyst

Seth Schoen, Senior Staff Technologist

Adam Schwartz, Senior Staff Attorney

MARCH 8, 2017

Table of Contents

Authors: Sophia Cope, Amul Kalia, Seth Schoen, Adam Schwartz
With assistance from: Hugh D'Andrade, Gennie Gebhart, Cooper Quintin, Rainey Reitman, Corynne McSherry
A publication of the Electronic Frontier Foundation 2017

EXECUTIVE SUMMARY

The U.S. government reported a five-fold increase in the number of electronic media searches at the border in a single year, from 4,764 in 2015 to 23,877 in 2016.[1] Every one of those searches was a potential privacy violation. Our lives are minutely documented on the phones and laptops we carry, and in the cloud. Our devices carry records of private conversations, family photos, medical documents, banking information, information about what websites we visit, and much more. Moreover, people in many professions, such as lawyers and journalists, have a heightened need to keep their electronic information confidential. How can travelers keep their digital data safe?

The U.S. Constitution generally places strong limits on the government's ability to pry into this information. At the U.S. border, however, those limits are not as strong, both legally and practically. As a matter of the law, some legal protections are weaker – a fact EFF is working to change. As a matter of practice, border agents may take a broad view of what they are permitted to do. Border agents may attempt to scrutinize the content stored on your phones, laptops, and other portable electronic devices. They may try to use your devices as portals to access your cloud content, including electronic communications, social media postings, and ecommerce activity. Moreover, agents may seek to examine your public social media postings by obtaining your social media identifiers or handles. As of this writing, the federal government is considering requiring disclosure from certain foreign visitors of social media login credentials, allowing access to private postings and "friend" lists.

1 Gillian Flaccus, *Electronic media searches at border crossings raise worry,* Associated Press (Feb. 18, 2017), http://bigstory.ap.org/article/6851e00bafad45ee9c312a3ea2e4fb2c/electronic-media-searches-border-crossings-raise-worry.

This guide (updating a previous guide from 2011[2]) helps travelers understand their individual risks when crossing the U.S. border, provides an overview of the law around border search, and offers a brief technical overview to securing digital data.

As an initial matter, readers should note that *one size does not fit all.* We are deeply concerned by invasive and even abusive practices of some border agents, and we are well aware of the serious consequences some travelers may face if they run afoul of a border agent. Many groups, including EFF, are working to establish clear legal protections to help alleviate that fear. In the meantime, however, we know that some travelers will want to take a highly conservative approach, while others will be less concerned. This guide is intended to help you make informed choices according to your situation and risk-tolerance.

Part 1 identifies the **risk assessment factors** that all travelers should consider (such as immigration status, travel history, and the data stored on the device) and the **potential actions** that travelers can take to secure their digital privacy at the U.S. border. Those actions include:

- ***Before your trip.*** Travelers should decide whether they can reduce the amount of digital information that they carry across the border. For example, they may leave certain devices at home, use temporary devices, delete content from their devices, or shift content to the cloud. Travelers should protect the information they do carry over the border. Most importantly, they should use full-disk encryption and backup their data somewhere else. Also, shortly before arriving at the border, travelers should power off their devices, which will resist a variety of high-tech attacks against encryption. Travelers should not rely solely on fingerprint locks, which are less secure than passwords.

- ***At the U.S. border.*** Agents may ask travelers to unlock their devices, provide their device passwords, or disclose their social media information. This presents a no-win dilemma. If a traveler complies, then the agents can scrutinize and copy their sensitive digital information. If a traveler declines, then the agents can seize their devices, subject the traveler to additional questioning and detention, and otherwise escalate the encounter.

  Border agents cannot deny a U.S. citizen admission to the country. However, if a foreign visitor declines, an agent may deny them entry. If a lawful permanent

2 *Defending privacy at the U.S. border: A guide for travelers carrying digital devices* (Dec. 2011), https://www.eff.org/files/eff-border-search_2.pdf.

resident declines, agents may raise complicated questions about their continued status as a resident.

Your response to this dilemma may vary according to your risk assessment. However, all travelers should stay calm and respectful, should not lie to border agents or physically obstruct them, and should plan for this dilemma ahead of time. Try to document or politely ask for the names, badge numbers, and agencies of the government officers you interact with.

- ***After your trip.*** If you feel that U.S. border agents violated your rights by searching or seizing your digital devices or online accounts, please contact EFF at borders@eff.org. Also, write down everything that happened as soon as possible.

Part 2 provides a primer on the law and policies related to border search of digital devices to help you understand the broader legal context. In particular, we address:

- ***Your rights at the border.*** Compared to people and police in the interior of the country, border agents have more power and people crossing the border have less privacy. But the border is not a Constitution-free zone. The powers of border agents are tempered by the First Amendment (freedom of speech, association, press, and religion), the Fourth Amendment (freedom from unreasonable searches and seizures), the Fifth Amendment (freedom from compelled self-incrimination), and the Fourteenth Amendment (freedom from discrimination).
- ***Government policies and practices at the border.*** For many years, the federal government has asserted broad powers at the border to search and seize travelers' digital information. These intrusions are growing in frequency and intensity.

Finally, **Part 3** is a primer on the technology of privacy protection. To secure our digital lives, we often must rely on (and understand) encryption, passwords, effective deletion, and cloud storage. In Part 1, we highlight some of the ways you can use these tools and services to protect your privacy. Part 3 offers a deeper dive.

Want to learn more about surveillance self-defense? Since you are reading this guide, you may be interested in digital security in general, and not just while you are crossing international borders. If so, check out EFF's Surveillance Self-Defense guide.[3]

3 *Surveillance Self-Defense*, EFF, https://ssd.eff.org/.

Want to help EFF protect everyone's digital privacy at the border? Contact your U.S. senators and representatives, and ask them to support legislation requiring government officials to get a warrant from a judge based on probable cause of criminal activity before searching digital devices at the border. Also, please join EFF!

PART 1: DIGITAL PRIVACY GUIDE FOR TRAVELERS

In this section we highlight issues you should consider before you arrive at the border, and lay out options for protecting your privacy in light of your own risk assessment.

What is the Border?

According to the U.S. government, "the border" includes the land borders with Canada and Mexico, airports for international flights, and seaports for international cruises.[4] Travelers crossing the border will be inspected by U.S. Customs & Border Protection (CBP) officials, which may include an interview and examination of personal belongings. At 15 airports and one seaport (in Canada, the Caribbean, Ireland, and the United Arab Emirates), travelers will be inspected by CBP prior to departing the foreign country, rather than upon arrival in the United States.[5]

Risk Assessment Factors

A variety of factors can influence the precautions that travelers take at the U.S. border to protect their privacy. Here are a few things to consider.

Factors about You

1. **Citizenship, Residence, and Immigration Status**
   If you are a foreign visitor, you may be more easily denied entry into the country. If you are a lawful permanent resident, entry raises complicated questions about the government's ability to challenge your continued status as a resident. Thus, if you are not a U.S. citizen, refusing to comply with a border agent's demand that you unlock your device, provide your device password, or disclose your social media information may raise special concerns. That, in turn, may call for protective measures, or consultation with a lawyer, before you begin your trip.

4 U.S. Customs and Border Protection, *At Ports of Entry*, https://www.cbp.gov/border-security/ports-entry.

5 U.S. Customs and Border Protection, *Preclearance Locations*, https://www.cbp.gov/border-security/ports-entry/operations/preclearance.

2. **Travel History**
   If you have traveled to certain countries, such as those regarded by the U.S. government as connected to terrorism, drug trafficking, or sex tourism, it may draw additional scrutiny from border agents. Your frequency of international travel and the length of your trips may also inspire additional screening.

3. **Law Enforcement History**
   If you are subject to an ongoing or past investigation, have a prior conviction, or otherwise are under suspicion for any reason, you may be screened or questioned more intensively.

4. **Tolerance for Hassle From Border Agents**
   How willing are you to risk a potential confrontation with border agents or delays in your travel plans? Your answer may affect your decision on whether to comply with an agent's demand that you unlock your device, provide your device password, or disclose your social media information.

5. **Interest in Advocating for Your Privacy**
   If you are philosophically opposed to intrusive border searches, you may feel that the importance of asserting your rights may outweigh the risk of having your devices seized, being extensively questioned, missing a flight, or otherwise being detained. If so, you should still educate yourself so you can be an effective advocate.

Factors About Your Data and Devices

1. **Sensitivity of the Data**
   All people need to consider the risk that the government may access their sensitive information. If you are a journalist, attorney, doctor, or other professional, you may have a special responsibility to safeguard your data.

2. **Seizure of the Device**
   Refusing to grant access to your phone may result in the government choosing to seize it. Can you tolerate the financial costs and inconvenience of losing a device to the government for an indefinite period of time?

3. **Lost Access to Information on the Device**
   Have you made a backup of the data on the device? If not and it is seized, you will not have access to that information for the duration of the seizure.

4. **Importance of Access to Data While Traveling**
   Do you need all your personal data while traveling? If not, consider leaving your device—or certain devices—at home. Alternatively, consider removing data from your device, or storing it in the cloud so you can access it once you reach your destination. If you do need data on your device while traveling, take precautions to protect your data.

5. **Quality of Internet Access During Trip**
   Will you have access to fast and reliable Internet access while traveling? If so, you may be able to limit the amount of data you carry over the border by using a cloud service provider.

6. **Who Owns Your Device**
   Do you own your device? If not, consult with the person who does (such as your employer).

Keep these factors in mind as you consider the options discussed in the following section.

Before You Arrive at the Border

The right time to start protecting your digital privacy is before your trip, when you are at home or work and have more time and greater access to information and people who can help you get set up properly.

Please be aware, however, that taking some precautions may attract unwanted attention and scrutiny, even if the precautions otherwise succeed in protecting your information. For example, if detected by a border agent, the fact that you wiped your hard drive may prompt the agent to ask why you did so. Even traveling without devices or data that most travelers typically have could attract suspicion and questions.

One more caveat: in what follows we touch on the technology of privacy protection at a high level. If you would like further information on this topic (such as the challenge of secure deletion), please see Part 3.

Talk to Your Employer

For work-owned devices and those that contain work-related information, talk to your employer about data security before traveling. Some employers have policies and procedures that can help protect both travelers and sensitive data, including from threats beyond searches at the border. CBP agents may be more sympathetic to

travelers who truthfully state that the traveler does not have access to data or was prohibited by their employer from granting anyone access to it.

Minimize the Data That You Carry Across the Border

The simplest and most reliable precaution against border searches is to reduce the amount of information that you carry across the border.

1. **Leave Your Devices at Home or Work**
   If you can leave electronic devices at home or work (or, in some cases, send them separately through the mail),[6] border agents cannot examine them as part of your entry into the country.

2. **Use a Temporary Device**
   If you can obtain a device just for travel, you can avoid loading information on it that you do not need for your trip. Many businesses have adopted some form of this approach, both because of border search risks and because of theft and hacking risks that may be heightened during travel. Individuals can do the same.

   Mobile phones that use the GSM standard (ubiquitous in most countries) let you switch a SIM card from one phone to another, so you can choose to keep your phone number while using a temporary travel phone.

   Depending on your priorities, a Chromebook can make a particularly good travel laptop when traveling somewhere with decent Internet access. Several models are available for under $200 as of this writing; they focus on storing most information online and using Google's cloud services. Chromebooks minimize the data stored on the device itself and are particularly easy to clear or reset.

3. **Shift Content From Devices to Cloud Services**
   If you move information from your device to cloud services, you can minimize what you will actually have in your possession as you cross the border.

   This can be a good approach, but we offer three cautions.

6 Objects sent through the mail are also subject to customs inspection, and it is possible, though unlikely, that customs inspectors will try to copy or search items that you ship. So, sending devices in the mail may protect you from some questions about those devices at the border, but will not always protect your devices from being searched.

First, storing data in the cloud carries its own risks. For example, border agents and other government officials may try to search your cloud data without your knowledge by dealing directly with the service provider. The good news: such demands are typically subject to greater legal safeguards than a border search.[7]

Second, border agents may ask you specifically about online accounts. If proposals being floated as of this writing are adopted, they may even ask some travelers for usernames and passwords in order to access the data themselves. Depending on your risk factors, the consequences of saying no can be significant.

Third, it can be difficult to thoroughly delete data from your devices. Even when you think you have "moved" data to the cloud, some of it could still actually be present on your devices. If agents seize your device and subject it to a forensic examination,[8] they may recover significant amounts of incompletely deleted data.

4. Delete Information From Your Devices

If you know you will not need certain information during a trip, you can delete it before crossing the border. If you want to remove *all* of your data, you can use third-party software or, sometimes, built-in options to "wipe" or "factory reset" a device to a blank or pristine state where no user data is readily accessible. However, border agents may find it suspicious if they realize that you have deleted some or all of your data before crossing the border.

In addition, it can be difficult to delete information securely in a way that leaves no traces. **Please see Part 3 for more information on securely wiping your device.**

5. Use Private Browsing Mode

Most browsers offer a private browsing mode. In this mode, the web browser avoids saving browsing history to the hard drive at all. Files are also not saved to the disk cache and so the forensic footprint of things you do online is reduced.[9]

---

7 Electronic Communications Privacy Act, 18 U.S.C. § 2703; *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (probable cause warrant needed to obtain emails from online service provider).

8 Forensic exams use special tools to search devices. In some but not all forensic exams, the tools access or locate information that is not normally visible or quickly apparent, such as deleted files or metadata.

9 Not all implementations of private browsing mode can hide 100% of web activity from forensic examination, because of issues like swap space, where information in the computer's memory may be saved to disk automatically.

Private browsing mode is not a way of clearing your browsing history after-the-fact. And clearing your browsing history may still leave the information vulnerable to forensic recovery by CBP officials. Rather, to get this benefit, you have to regularly use private browsing mode whenever you browse the web.

6. **Digital Cameras**
   Border agents may demand to look through the photos or videos on your cameras or phones. Most cameras do not come with encryption, so there are no convenient technical means that would prevent this kind of inspection.

   If you do not want border agents to see your photos or videos, the simplest approach is to delete them or move them to a secured laptop or cloud storage. You should be aware that forensic examination can typically recover deleted photos, unless the storage media has been securely wiped.

Protect What You Carry Over the Border

Whether or not you plan to cooperate with border agents' demands, you should take two basic precautions: make **backups** and use **encryption**. Backups prevent your data from being lost if your device is seized, stolen, or broken—risks that are significantly heightened during international travel. Encryption prevents others from accessing your data in certain scenarios. Even if you are prepared to unlock your devices or provide the passwords, using encryption still prevents your devices from being searched or examined without your knowledge.

1. **Backup Your Data**
   Travelers should always have backups of their data. Your need to access the backup during your trip may vary, so depending on your situation, you may want to leave a backup at home or at work as a fallback option, or you may want an online backup that can be accessed during your travel. Backups are especially important for password managers as they grant you access to your online accounts.

   You can make backups of a phone or tablet onto a computer (often over a USB, Thunderbolt, or Firewire cable). You can make backups of a computer onto an external hard drive, or sometimes other media like DVD-R or a home or office file server.

In places with fast Internet access, online backups have become the most popular option for backing up all kinds of devices. They are discussed in Part 3.

2. **Encrypt Your Data**

   Encryption is an important technology to protect all kinds of data from unauthorized access in all kinds of circumstances. We focus here on encryption of stored data on devices (rather than end-to-end encryption of communications). More details are included in Part 3, including encryption tools that may be available for your device.

   People often decide to "set a password" on their device in order to protect their data. This intuition is right, but the details matter significantly. Not all ways of "setting a password" provide the same kind of protection, and many do not involve any encryption at all. For strong data protection, you need to ensure that your password will actually encrypt the hard drive content, rather than only controlling access to the device.

   A **screen-lock password** or **user account password** is enforced by the operating system code and only controls access to the device. The operating system is configured to ask for the password and will not allow access unless the right one is provided. But the data is still simply present on the hard drive in unencrypted form. Forensic tools can easily bypass such passwords and access the unencrypted hard drive content. CBP, ICE, and other federal law enforcement agencies have staff with training and access to these tools.

   By contrast, a password used for **storage encryption** uses mathematical techniques to scramble the data on the hard drive so it is unintelligible without the right cryptographic key. This mathematical protection works independently of the operating system software. A different device or software program cannot just decide to allow access, because *no device or software program* can make any sense of the data without the right key.

   Fortunately, modern phone, tablet, and computer systems usually come with comparatively easy-to-use **"full-disk" storage encryption** features that can encrypt the full contents of the device with a password that will be required when the device is first powered on. **Using these tools is the most fundamental security precaution for travelers who have sensitive information on their devices and are concerned about losing control of them —not just at a border crossing, but at any point during a trip.**

3. **Use Strong Passwords**

   Strong passwords are critical for encryption. A border agent once accessed a traveler's digital devices by correctly guessing that the traveler used her birthday as her. [10] Even a random password that's too short or predictable could be easy for someone to crack by machine, allowing them to decrypt data on a seized device. So you should create a password that is long and unpredictable—but also memorable. One approach is a phrase made of several words randomly selected by a computer or by rolling dice. More information about strong passwords is in Part 3.

4. **Power Off Your Devices**

   We recommend that you power off all of your devices before you arrive at a border checkpoint. This will resist a variety of high-tech attacks against encryption that only work when a device is already powered on. For some mobile devices, powering off also resets the device to a higher-security state that requires a password to unlock, which may not be true in day-to-day use.

5. **Do Not Rely Solely on Biometric Keys**

   Many phones and tablets, and some laptops, can be locked with a biometric feature like a fingerprint. While this can be a convenient security precaution, it may not offer the same security and legal benefits as a password that you memorize. Before arriving at the border, make sure that your device requires a password to decrypt, and that your device has been powered off.

6. **Traveling Without Knowledge of Your Passwords**

   You can arrange *not to know* information necessary to decrypt your device, including your password. If so, you cannot be compelled to divulge that information. This would provide the highest possible level of protection for devices that you carry across the border. Also, it may provide a disincentive to agents to try to force you to reveal what you do not know. However, it may also cause agents to escalate if they find it suspicious that you are carrying a device you cannot "unlock."

   If you take this approach, you have a few options. For example, you could generate a new random password that is too long for you to remember, change your password to the new one, and then give this password to someone else, send it via a different channel, or store it online where you can only retrieve it once you have Internet access. A variation on this idea is to tell it to a lawyer, so that nobody can retrieve it without getting your lawyer involved.

10 *United States v. Lopez*, 2016 WL 7370030 (S.D. Cal. 2016).

These approaches are probably most useful to people whose highest priority is protecting their information: while you cannot be forced to unlock a device, border agents may still seize the device or escalate the situation. Again, not knowing your password is very unusual and agents may find it suspicious or difficult to believe. If you choose this approach, you may wish to have some information to substantiate the fact that you really don't know your password, and recognize that this may still not satisfy the agents.

7. **Do Not Try to Hide Data on Your Devices**
   Some people have proposed technical means of hiding data on a device so that it is not apparent to a border agent. For example, a "hidden volume" feature may make different data appear depending on which password is entered. Other possible techniques may make searches harder or less fruitful, make data available under some conditions but not others, make data self-delete, or make it less apparent where data is kept, who can access it, or what its nature is.

   We appreciate and respect technologists' efforts to find ways to help travelers protect their data. However, w**e recommend against using methods that may be, or even appear to be, calculated to deceive or mislead border agents about what data is present on a device.** There is a significant risk that border agents could view deliberately hiding data from them as illegal. Lying to border agents can be a serious crime, and the agents may take a very broad view of what constitutes lying.[11] We urge travelers to take that risk very seriously.

Social Media and Online Accounts

If you are reluctant to have the government review what you post on social media, you can change your social media privacy settings (at least temporarily) to make your posts not viewable by the general public.

On your devices, you should consider logging out of browsers and apps that give you access to online content, and removing saved login credentials. This will prevent border agents, without your knowledge, from using your devices to access your private online

11 18 U.S.C. § 1001(a)(2) (it is a crime to "knowingly and willfully… make[] any materially false, fictitious, or fraudulent statement or representation" in "any matter" within government jurisdiction). See also 18 U.S.C. § 1001(a)(1) (same for a person who knowingly "falsifies, conceals, or covers up by any trick, scheme, or device a material fact"); 18 U.S.C. § 1001(a)(3) (same for a person who knowingly "makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry"); 18 U.S.C. § 1519 (same for whoever knowingly "alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation").

information. You could also temporarily uninstall mobile apps, and clear browser history, so that it is not immediately apparent which online services you use.[12]

Note that while certain messaging apps provide end-to-end encryption, if a border agent has access to your app, they will be able to see your messages in plain text *within the app itself.*

When You Are at the Border

The hardest part of protecting your privacy at the border is deciding how to respond if a border agent demands that you help them invade your digital privacy.

If you are a U.S. citizen, border agents cannot stop you from entering the country, even if you refuse to unlock your device, provide your device password, or disclose your social media information. However, agents may escalate the encounter if you refuse. For example, agents may seize your devices, ask you intrusive questions, search your bags more intensively, or increase by many hours the length of detention. If you are a lawful permanent resident, agents may raise complicated questions about your continued status as a resident. If you are a foreign visitor, agents may deny you entry.

Unjustified escalation may violate the law and, as discussed in the next section, you may have some recourse after you exit. However, some travelers may want to avoid any risk of escalation if they can.

What to Expect

When you arrive at the border, agents may seek access to your device by demanding that you type in your password, tell them your password, or (if you use a fingerprint key) press your finger to the sensor. This will give the agents access to information you store on your device. It will also give them access to information you store in the cloud, including private communications, if that information is accessible through your device via apps or a browser. Border agents may also ask you to disclose your social media identifiers, which would allow them to scrutinize your public social media content, even if they do not have access to your devices. If proposals being floated as of this writing are adopted, border agents may ask for your social media login credentials (usernames and passwords), which would allow them to scrutinize your private social media content.

12 Agents could still ask about your online accounts even when what you use is not apparent from your devices. Also, a forensic examination of a seized device will usually reveal online activity even if you have deleted apps or cleared history.

Basic Rules for Everyone

First, decide how you will respond to border agents' demands before you arrive at the border. Make this decision holistically, in light of your unique risk assessment factors, along with all of the other before-you-arrive decisions discussed above.

Second, stay calm and respectful. Staying calm will help you make better decisions. Also, if you get emotional or disrespectful, some agents may escalate the encounter. CBP, in turn, pledges to treat travelers with "courtesy, dignity and respect."[13]

Third, do not lie to a border agent. It is a crime to make a false statement to a law enforcement official who is asking you questions as part of their job.[14]

Fourth, do not physically interfere with a border agent. This includes complying with demands to open your luggage or hand over your digital devices. Border agents may legally inspect the physical aspects of a device—for example, the battery compartment or inside a case—to ensure that it does not contain contraband such as drugs or explosives.[15] If you do physically interfere, border agents may respond with physical force.

Fifth, if you have any problems, try to document the names, badge numbers, and agencies of the officers you interact with at the border. If you decide later to file a complaint about the way the officers treated you, it will be easier to do so if you know who they were. Also, if officers seize your digital devices, politely demand a property receipt (Customs Form 6051D).

Try to Avoid Implicit "Consent"

Law enforcement officials often try to persuade civilians to consent to searches. Once the civilian consents, it can be harder to challenge the search in court.

Sometimes law enforcement officials achieve so-called "consent" by being vague about whether they are asking or ordering a civilian to do something. You can try to dispel this ambiguity by inquiring whether border agents are asking you or ordering you to unlock your device, provide your device password, or disclose your social media information. If an agent says it is a request only, you might politely but firmly decline to comply with the request.

---

13 U.S. Customs and Border Protection, Securing America's Borders: The CBP Screening Process, https://www.cbp.gov/sites/default/files/documents/securing-americas-borders_0.pdf.

14 18 U.S.C. § 1001(a); 18 U.S.C. § 1519.

15 *See Riley v. California*, 134 S. Ct. 2473, 2485 (2014).

What Could Happen When You Comply With an Order?

If you do comply with an order to unlock your device, provide your device password, or disclose your social media information, several things may occur.

- Border agents may scrutinize all of the content stored in your device, manually or with powerful forensic software.
- Border agents may scrutinize all of the cloud content accessible through your device, including private content and communications.
- Border agents may copy and store all of this content for their later use.[16]
- If you later bring a legal challenge to the search of your device, the government may defend its actions by saying you consented to the search.

If You Comply With an Order, Should You State That It Is Under Protest?

If you elect to comply with a border agent's order to unlock your device, provide your password, or disclose your social media information, you can inform the agent that you are complying under protest and that you do not consent. If you later assert a legal challenge, this may help you defeat the government's claim that you consented to the search.

What Could Happen if You Refuse to Comply With an Order?

If you refuse to comply with an order to unlock your device, provide your password, or disclose your social media information, several things may occur.

- The border agent may escalate the encounter.
- Border agents may seize your devices. Then CBP and ICE agents may attempt to access your digital data without your assistance. Even if they cannot decrypt your devices, they may be able to copy the encrypted contents of your devices. If they later obtain your passwords, or find vulnerabilities in the encryption, they may be able to decrypt their copies. The government's scrutiny of your devices may take months. During this time, you may need to purchase replacement devices, and you will not have access to the information on the devices.
- You may be flagged for heightened screening whenever you cross the U.S. border in the future.

16 There have been reports that CBP agents are storing device passwords for use the next time a traveler crosses the border. See, e.g., Kaveh Waddell, *How long can border agents keep your email password?* The Atlantic (Feb. 27, 2017), https://www.theatlantic.com/technology/archive/2017/02/border-agents-personal-information/517962/.

- The border agent may let you pass through without further interference.

Should You Attempt to Persuade the Agents to Withdraw Their Order?

Some travelers may attempt to avoid this no-win dilemma by trying to persuade the border agent to withdraw their demand to unlock a device, provide a device password, or disclose social media information. For example, the traveler may object that the information is especially sensitive, such as attorney-client correspondence or journalistic sources. Likewise, the traveler may object that the devices belong to their employer, and that the agent should speak to their employer's lawyers if they want to search the devices.

This tactic may work for some travelers. But it carries risks. For example, it may induce a conversation with the agent about the contents of your device, which carries the risk that you will make statements against your interests.

After You Leave the Border

If you believe that border agents violated your digital rights at the border, please contact EFF at borders@eff.org.

Make a Record of What Happened

If you are unhappy with how border agents treated you, then you should write down everything you remember about the event as soon as you can. This may help you later if you choose to challenge the agents' actions. You should also try to identify witnesses.

You may also want to ask the government for its written records about you and your encounter at the border. Anyone can do this with the Freedom of Information Act.[17] U.S. citizens and legal permanent residents also can do this with the Privacy Act.[18]

The CBP and ICE websites for records requests are:

- https://www.cbp.gov/site-policy-notices/foia
- https://www.ice.gov/foia/request

17 5 U.S.C. § 552. There are several online tools to help write FOIA requests. See, e.g., *Reporters Committee for Freedom of the Press*, iFOIA.org; Muckrock, File a Request, https://www.muckrock.com/foi/create/.

18 5 U.S.C. § 552a.

Change Your Passwords and Login Credentials

If you gave your device passwords or account login credentials to a border agent, then the government has continuing power over your digital information. For example, there are reports that CBP agents store device passwords for use the next time a traveler crosses the border.[19] If you aren't comfortable with that continuing power, you should change your passwords and credentials.

Government Offices That May Help You

You may wish to file a complaint with, or seek help from, the government. However, you would benefit from speaking with a lawyer before doing so, especially if it is possible that you will file a lawsuit about your experience at the border.

- You can file a complaint with CBP: https://help.cbp.gov/app/forms/complaint
- You can file a complaint with DHS's Office of Civil Rights and Civil Liberties: https://www.dhs.gov/file-civil-rights-complaint
- If border agents have repeatedly referred you to secondary screening over the course of several international trips, and you think you may be on a government watchlist or misidentified as someone else who is listed, you can seek help from **DHS's Traveler Redress Inquiry Program (TRIP):** https://www.dhs.gov/dhs-trip

19 See, e.g., Kaveh Waddell, *How long can border agents keep your email password?* The Atlantic (Feb. 27, 2017), https://www.theatlantic.com/technology/archive/2017/02/border-agents-personal-information/517962/.

PART 2: CONSTITUTIONAL RIGHTS, GOVERNMENT POLICIES, AND PRIVACY AT THE BORDER

In this section we address the legal framework that allows, and limits, border searches and seizures. The law in this area is evolving and adapting, imperfectly, to technological changes, creating uncertainty for travelers and government agents alike. EFF is fighting in the courts and in legislatures to resolve that uncertainty and ensure that travelers can count on strong protections for their digital rights at the border.[20]

This primer provides general information only. When in doubt, you should consult with a lawyer.

The Law of Border Searches and Seizures

As a general principle, government agents at the U.S. border enjoy more power than police officers working in the American interior. Most of the time, border agents exercise these powers on travelers arriving in the United States, but they sometimes apply them to travelers *leaving* the United States as well.

However, the U.S. border is not a Constitution-free zone. The powers of border agents are tempered by our Fourth Amendment right to digital privacy, our First Amendment rights to speak and associate privately and to gather the news, our Fifth Amendment right to freedom from self-incrimination, and our Fourteenth Amendment right to freedom from discrimination.

20 *United States v. Arnold*, No. 06-50581 (9th Cir.), *amicus* brief of EFF (June 10, 2008), https://www.eff.org/document/amicus-brief-united-states-v-arnold; *United States v. Cotterman*, No. 09-10139 (9th Cir.), *amicus* brief of EFF (Sept. 19, 2011), https://www.eff.org/files/filedcottermanamicusbrief_0.pdf; *United States v. Saboonchi*, No. 15-4111 (4th Cir.), *amicus* brief of EFF (Sept. 10, 2015), https://www.eff.org/document/eff-saboonchi-amicus-brief.

The Fourth Amendment at the Border: Digital Privacy

The Default Constitutional Privacy Rule

The Fourth Amendment to the U.S. Constitution is the primary protector of individual privacy against government intrusion. The Fourth Amendment prohibits "unreasonable" searches and seizures by the government.[21] The default rule to ensure that a search or seizure is reasonable is that law enforcement officials must first obtain a "probable cause" warrant.[22] This means that the officer must present preliminary evidence to a judge that shows that the thing to be searched or seized likely contains evidence of illegal activity.

The Border Search Exception

The Supreme Court has interpreted the Fourth Amendment to include a "border search exception" to the standard warrant and probable cause requirements. The Court has held that the government has an interest in protecting the "integrity of the border"[23] by enforcing the immigration and customs laws.[24] For "routine" searches, such as those of luggage and other common possessions presented at the border, the Supreme Court concluded that this specific governmental interest outweighs an individual's privacy interests. The Court presumes that warrantless and suspicionless border searches are critical to:

1. Ensuring that travelers entering the U.S. have proper authorization and documentation;
2. Enforcing the laws regulating the importation of goods into the U.S., including duty requirements;

---

21 *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006) ("the ultimate touchstone of the Fourth Amendment is 'reasonableness'").

22 *Katz v. U.S.*, 389 U.S. 347, 357 (1967) (warrantless searches "are per se unreasonable").

23 *U.S. v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

24 *See, e.g., Boyd v. United States,* 116 U.S. 616, 623 (1886) (power to identify "goods liable to duties and concealed to avoid the payment thereof," but not for "seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him"); *Carroll v. U.S.*, 267 U.S. 132, 154 (1925) (power to require a traveler "to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in"); *Almeida-Sanchez v. U.S.*, 413 U.S. 266, 272 (1973) (power to exclude aliens); *U.S. v. Ramsey*, 431 U.S. 606, 620 (1977) (power "to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country"); *U.S. v. Montoya de Hernandez*, 473 U.S. 531, 537, 544 (1985) (power "to regulate the collection of duties and to prevent the introduction of contraband" or "anything harmful" such as "communicable diseases, narcotics, or explosives").

3. Preventing the entry of harmful people (e.g., terrorists) and harmful items (i.e., contraband) such as weapons, drugs, and infested agricultural products.[25]

In sum, the border search exception provides that **"routine" searches at the border do not require a warrant or any individualized suspicion that the thing to be searched contains evidence of illegal activity.[26]**

The Exception to the Exception: "Non-Routine" Searches

The Supreme Court has also recognized that not all border searches are "routine." Some of them are "highly intrusive" and impact the "dignity and privacy interests" of individuals,[27] or are carried out in a "particularly offensive manner."[28] At minimum, such non-routine border searches require that border agents have some level of *individualized suspicion* about the traveler.

"Individualized suspicion" is a legal term that means that the border agent has a factual reason to believe a specific person is involved in criminal activity.

Thus, for example, the Supreme Court held that disassembling a gas tank is "routine" and so a warrantless and suspicionless search is permitted.[29] However, detaining a traveler until they have defecated to see if they are smuggling drugs in their digestive tract is a "non-routine" search that requires "reasonable suspicion" that the traveler is a drug mule.[30] Likewise, lower courts have held that body cavity searches and strip searches are "non-routine" and also require reasonable suspicion.[31]

Border Searches of Digital Devices

Given that digital devices like smartphones and laptops contain highly personal information and provide access to more highly personal information stored in the cloud, are border searches of digital devices "routine?" There is some legal uncertainty at the moment, but we believe the final answer is **no**.

---

25 *See, e.g.*, Chad Haddal, *Border Security: Key Agencies and Their Missions* 2 (2010), https://www.fas.org/sgp/crs/homesec/RS21899.pdf ("CBP's mission is to prevent terrorists and terrorist weapons from entering the country, provide security at U.S. borders and ports of entry, apprehend illegal immigrants, stem the flow of illegal drugs, and protect American agricultural and economic interests from harmful pests and diseases").

26 *U.S. v. Montoya de Hernandez,* 473 U.S. 531, 537 (1985).

27 *U.S. v. Flores-Montano*, 541 U.S. 149, 152 (2004).

28 *U.S. v. Ramsey*, 431 U.S. 606, 618 n.13 (1977).

29 *U.S. v. Flores-Montano,* 541 U.S. 149, 155 (2004).

30 *U.S. v. Montoya de Hernandez,* 473 U.S. 531, 541 (1985).

31 *U.S. v. Ogberaha*, 771 F.2d 655 (2d Cir. 1985) (body cavity search); *U.S. v. Gonzalez-Rincon*, 36 F.3d 859 (9th Cir. 1994) (strip search).

In *U.S. v. Cotterman* (2013), the U.S. Court of Appeals for the Ninth Circuit held that border agents need reasonable suspicion of illegal activity (at least within the authority of border agents to investigate) before they could conduct a *forensic* search, aided by sophisticated software, of the defendant's laptop. Unfortunately, the court also held that a *manual* search of a digital device is "routine" and so a warrantless and suspicionless search is "reasonable" under the Fourth Amendment.[32]

One year later, however, in *Riley v. California* (2014), the Supreme Court held that the police had to obtain a probable cause warrant to search the cell phone of an individual under arrest. The police had argued that the warrantless and suspicionless cell phone search was permissible as a "search incident to arrest," the same way it would be possible for the police to search the pockets or wallet of an arrestee for drugs or weapons. In short, the police invoked an exception to the Fourth Amendment similar to the border search exception. Rejecting that argument, the Court held that "a warrant is generally required before such a search, even when a cell phone is seized incident to arrest."[33]

No appellate court has yet applied the *Riley* decision in the border context, but the Supreme Court itself has recognized that the search-incident-to-arrest exception invoked by the government in *Riley* is similar to the border search exception.[34] Thus, **we believe that all border searches of digital devices should require a probable cause warrant.**

In both the *Cotterman* and *Riley* cases, courts stressed the significant privacy interests in all the data modern digital devices contain—call logs, emails, text messages, voicemails, browsing history, calendar entries, contact lists, shopping lists, personal notes, photos and videos, geolocation logs, and other personal files. Digital devices typically cover many years of information and include the most intimidate details of a person's life. The Supreme Court in *Riley* rejected the notion that cell phones are the same as physical items: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon" just because both are "ways of getting from point A to point B."[35]

Both courts also raised special concerns about the government accessing cloud content via digital devices. The Ninth Circuit in *Cotterman* stated:

---

32 *U.S. v. Cotterman*, 709 F.3d 952, 967 (9th Cir. 2013).

33 *Riley v. California*, 134 S. Ct. 2473, 2493 (2014).

34 Prior to *Riley,* the Supreme Court noted the similarity between the border search exception and the search-incident-to-arrest exception. *U.S. v. Ramsey*, 431 U.S. 606, 621 (1977).

35 *Riley v. California*, 134 S. Ct. 2473, 2488 (2014).

> With the ubiquity of cloud computing, the government's reach into private data becomes even more problematic. In the "cloud," a user's data, including the same kind of highly sensitive data one would have in "papers" at home, is held on remote servers rather than on the device itself. The digital device is a conduit to retrieving information from the cloud, akin to the key to a safe deposit box. Notably, although the virtual "safe deposit box" does not itself cross the border, it may appear as a seamless part of the digital device when presented at the border. [36]

Similarly, the Supreme Court in *Riley* stated that using the search incident to arrest exception to justify searching files stored in the cloud "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[37]

Therefore, to the extent that border searches of digital devices access cloud data, the privacy interests are even more significant. Given these interests, the border search exception should not apply.[38]

Interior Checkpoints

Border agents may establish permanent checkpoints on roads that are miles away from the international border, where agents may stop motorists for brief questioning, even in the absence of any individualized suspicion.[39] However, border agents at these checkpoints cannot search a car without probable cause.[40] Likewise, border agents at these checkpoints should not be able to search a digital device without probable cause.

The First Amendment at the Border: Freedom to Privately Speak, Associate, Acquire Information, and Gather News

When border agents scrutinize the massive volume of sensitive information in our digital devices, they infringe on our First Amendment rights in at least four distinct

36 *U.S. v. Cotterman,* 709 F.3d 952, 965 (9th Cir. 2013).

37 *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).

38 Districts courts have also been considering *Cotterman* and *Riley*. *See, e.g., U.S. v. Saboonchi*, 48 F. Supp. 3d 815 (D. Md. 2014); *U.S. v. Martinez,* 2014 WL 3671271 (S.D. Cal. 2014); *United States v. Kim*, 103 F. Supp. 3d 32 (D.D.C. 2015); *U.S. v. Kolsuz*, 185 F. Supp. 3d 843 (E.D. Va. 2016); *U.S. v. Caballero*, 178 F. Supp. 3d 1008 (S.D. Cal. 2016).

39 *United States v. Martinez-Fuert*e, 428 U.S. 543, 562 (1976).See generally ACLU, The Constitution in the 100-mile Border Zone, https://www.aclu.org/other/constitution-100-mile-border-zone.

40 *United States v. Ortiz*, 422 U.S. 891 (1975). *See also Almeida-Sanchez v. United States*, 413 U.S. 266 (1973) (border agents conducting roving patrols near the border need probable cause to search a car).

ways.

First, border searches of digital devices may intrude on the First Amendment right to speak anonymously. This includes the right to use a pseudonymous social media handle.[41] Border agents will unmask anonymous speakers by linking the passport-verified identities of travelers to pseudonyms revealed through device searches or disclosure of social media handles.

Second, border searches of digital devices may disclose private membership in expressive associations, like being part of a political group or social club. The First Amendment protects the right to join together with other people to advance a shared message.[42] This includes the right to privately participate in an expressive association, for example, in an advocacy organization with a private membership list.[43]

Third, border searches of digital devices may reveal the private decisions that travelers make to acquire expressive materials, such as books and movies. The First Amendment protects the right to receive information,[44] and to do so without telling the government what we are reading and watching.[45]

Fourth, border searches of digital devices may disclose confidential journalistic sources and work product. This burdens the First Amendment right to freedom of the press, specifically the ability to maintain the integrity and independence of the newsgathering process. The Supreme Court has said that journalists are not "without

41 *McIntyre v. Ohio Elections Comm'n,* 514 U.S. 334 (1995); *Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088 (W.D. Wash. 2001). *See generally EFF, Anonymity,* https://www.eff.org/issues/anonymity.

42 *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 907 (1982).

43 *NAACP v. Alabama*, 357 U.S. 449 (1958).

44 *See, e.g., Virginia Pharmacy Bd. v. Virginia Consumer Council*, 425 U.S. 748, 757 (1976) (protecting the right to advertise, based in part on the consumer's "reciprocal right to receive the advertising" in order to make informed decisions); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (protecting the right to possess obscene materials at home, because "the right to receive information and ideas, regardless of their social worth . . . is fundamental to our free society"); *Lamont v. Postmaster Gen.*, 381 U.S. 301, 308 (1965) (Brennan, J., concurring) (protecting the "right to receive" foreign publications, because "[i]t would be a barren marketplace of ideas that had only sellers and no buyers"); *Martin v. City of Struthers,* 319 U.S. 141, 143 (1943) (protecting door-to-door leafleting, based in part on "the right of the individual householder to determine whether he is willing to receive her message"); *Conant v. Walters,* 309 F.3d 629, 643 (9th Cir. 2002) (protecting a patient's "right to receive" information from a physician about medical marijuana, because "the right to hear and the right to speak are flip sides of the same coin").

45 *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154 (W.D. Wash. 2010); *In re Grand Jury Investigation*, 706 F. Supp. 2d 11 (D.D.C. 2009); *In re Grand Jury Subpoena*, 246 F.R.D. 570 (W.D. Wis. 2007); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002) (en banc); *In re Grand Jury Subpoena to Kramerbooks*, 26 Media L. Rep. 1599 (D.D.C. 1998).

constitutional rights with respect to the gathering of news or in safeguarding their sources."[46]

To protect these First Amendment interests, border agents should be required to get a warrant supported by probable cause before searching digital devices. Indeed, when police officers demand records from booksellers, for example, about the purchases of individual customers, courts have held that an ordinary probable cause warrant is not enough. Instead, the First Amendment requires police to additionally show a compelling need, the exhaustion of less restrictive investigative methods, and a substantial nexus between the information sought and the investigation.[47] Obviously, a device search is far more intrusive of First Amendment rights than disclosure of what books a person buys at a single bookseller.

The reason for this protection is simple: government snooping will chill and deter First Amendment activity. Rather than risk border agent examination, many people will refrain from anonymous speech, from private membership in political groups, or from downloading certain reading material. This is especially true for people who belong to unpopular groups, who espouse unpopular opinions, or who read unpopular books. Likewise, confidential sources who provide invaluable information to the public about government or corporate malfeasance may refrain from whistleblowing if they fear journalists cannot protect their identities during border crossings.

Unfortunately some courts have rejected First Amendment challenges to border searches of digital devices.[48] Given the increasing amount of sensitive information

---

46 *Branzburg v. Hayes*, 408 U.S. 665, 709 (1972) (Powell, J., concurring). *See also, e.g., Zerilli v. Smith*, 656 F.2d 705 (D.C. Cir. 1981); *United Slates v. Cuthbertson*, 630 F.2d 139 (3d Cir. 1980). Protections for journalists' confidential sources and work product, often called a reporter's privilege, may also be found in federal common law and state laws, including statutes called "shield laws." *See, e.g., The Reporter's Privilege Compendium: An Introduction,* https://www.rcfp.org/browse-media-law-resources/guides/reporters-privilege/introduction.

47 Some courts have required enhanced First Amendment standards for search warrants for expressive materials. *See, e.g., Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002); *Quantities of Copies of Books v. State of Kansas*, 378 U.S. 205 (1964). Regarding the expressive materials of journalists specifically, it is clear that warrantless and suspicionless searches of digital devices at the border implicate free press rights. Should border agents ultimately be required to obtain a probable cause warrant, it is unclear whether the First Amendment would require the government to make an even higher showing before searching journalists' devices. *See Zurcher v. Stanford Daily*, 436 U.S. 547 (1978) (declining to require enhanced First Amendment standards for a newsroom search warrant, but requiring that Fourth Amendment standards be applied with "scrupulous exactitude"). However, the Privacy Protection Act, which was passed in response to *Zurcher,* prohibits the government from searching or seizing a journalist's materials without probable cause that the journalist has committed a crime. 42 U.S.C. § 2000aa. While the statute exempts border searches for the purpose of enforcing the customs laws, it does not exempt border searches for other purposes. 42 U.S.C. § 2000aa-5.

48 *Abidor v. Napolitano*, 990 F. Supp. 2d 260, 278 (E.D.N.Y. 2013); *United States v. Arnold*, 533 F.3d 1003, 1010 (9th Cir. 2008); *United States v. Ickes*, 393 F.3d 501, 505–07 (4th Cir. 2005).

easily accessible on and through our devices, and the increasing frequency and intensity of border searches of this information, we hope that other courts will rule differently in the future.

The Fifth Amendment at the Border: Freedom From Self-Incrimination

The Fifth Amendment guarantees that "no person shall be... compelled... to be a witness against himself." Statements and actions that qualify as bearing "witness" are called "testimonial." A person's statement or action is testimonial if it would disclose "the contents of [their] own mind."[49]

The best way to preserve your Fifth Amendment rights, given your own risk tolerance, is to politely but firmly decline to comply with a border agent's demand to unlock your device, provide your password, or disclose your social media information. Only a judge, and not a border agent, can decide whether the Fifth Amendment protects this information.

Passwords

At least one court has held that the Fifth Amendment confers an absolute right to refuse to provide one's password to unlock or decrypt a digital device [50] We believe that outcome was correct, for three reasons.

First, the act of entering a password into a device, or telling a border agent the password so the agent can enter it, will always be testimonial, because it will always expose the contents of the traveler's own mind.[51]

Second, when the data on a device is encrypted, the process of decryption is also testimonial, because it comprises the translation of otherwise unintelligible evidence into a form that investigators can understand.

Third, a foundation of the Fifth Amendment is "respect for the inviolability of the human personality and the right of each individual to a private enclave where [they] may lead a private life,"[52] and digital devices hold "the privacies of life."[53]

---

49 *United States v. Hubbell*, 530 U.S. 27, 34–35 (2000).

50 *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010).

51 *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (quashing a subpoena for computer passwords, because it would have required the suspect "to divulge through his mental process his password").

52 *Doe v. United States*, 487 U.S. 201, 212 (1988).

53 *Riley v. California*, 134 S. Ct. 2473, 2494–95 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

However, many courts have instead adopted a lesser, but still strong, test. Under this test, the government may compel a suspect to unlock their device only if the government can prove with "reasonable particularity" that it is a "foregone conclusion" that a "certain file" is stored on the device.[54] Border agents usually will not know what is stored on the device, so they can't compel you to disclose your password.

Sadly, other courts have adopted a weak test, under which the government need only show that the suspect knows the password.[55] Border agents will usually find it easier to show that a traveler knew the password of the device they carried, compared to showing that a particular suspect file was in that device.

Fingerprints

Properly construed, the Fifth Amendment *should* offer the same protections when people use fingerprints or other biometrics to secure their devices. The vast content of our devices ought to be part of the "private enclave" secured by the Fifth Amendment from self-incrimination.[56] Also, many consumers reasonably assume that their fingerprint lock is just as protective, legally and practically, as a password.

Unfortunately, some courts (though not all) have held that fingerprints, unlike passwords, are not part of the contents of our minds, and thus fall outside Fifth Amendment protection.[57] Moreover, police are developing technologies that can take a person's stored fingerprint from a government database and use it to unlock that person's phone.[58] Or an overzealous border agent may use force to press a traveler's finger to their phone. [59]

---

54 *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1344–47, 1349 n.28 (11th Cir. 2012). *See also SEC v. Huang*, 2015 WL 5611644, *2-3 (E.D. Pa. 2015) (denying a motion to compel unlocking because the SEC could not establish with "reasonable particularity" that documents sought were present). *Cf. In re Boucher*, 2009 WL 424718, *2-3 (upholding compelled unlocking where there the presence on the device of particular incriminating evidence was a foregone conclusion); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1235–37 (D. Colo. 2012) (same).

55 *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014); State v. Stahl, 206 So.3d 124 (Fla. Dist. Ct. App. 2016). *See also* Orin Kerr, *The Fifth Amendment Limits on Forced Decryption and Applying the "Foregone Conclusion" Doctrine*, Wash. Post (June 7, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine/.

56 *Doe v. U.S.*, 487 U.S. 201, 212 (1988).

57 *CompareState v. Diamond*, 2017 WL 163710 (Minn. Ct. App. 2017); *and Commonwealth v. Baust*, No. CR14-1439,2014 WL 10355635 (Va. Cir. Ct. 2014); *with In re Application for a Search Warrant,* No. 17-MC-00081 (N.D. Ill. Feb. 16, 2017).

58 Thomas Fox-Brewster, *$500 Fingerprint Clone Unlocked Murder Victim's Samsung S6*, Forbes (July 28, 2016), http://www.forbes.com/sites/thomasbrewster/2016/07/28/fingerprint-clone-hack-unlocks-murder-victim-samsung-s6-hacks-apple-iphone-galaxy-s7/.

59 Thomas Fox-Brewster, *Feds Walk Into a Building, Demand Everyone's Fingerprints to Open Phones*, Forbes (Oct. 16, 2016) (reporting a warrant from a federal judge in California that authorized police officers to push suspects' fingers into suspect devices),

Thus, fingerprints are less secure—both legally and technically—than passwords. You should consider using a password and not a fingerprint to lock or encrypt your digital devices.[60]

The First, Fifth, and Fourteenth Amendment Intersection at the Border: Freedom From Discrimination

Border agents may not decide whether to search or seize a traveler's digital devices, based on the traveler's religion, ethnicity, or similar characteristics.

The Equal Protection Clause of the Fourteenth Amendment prohibits the government from discriminating on the basis of factors such as race, religion, national origin, gender, and sexual orientation.[61] The Equal Protection Clause applies to the federal government through the Due Process Clause of the Fifth Amendment. Likewise, the Free Exercise and Establishment Clauses of the First Amendment prohibit religious discrimination.[62] Accordingly, law enforcement officials cannot discriminate on the basis of religion or similar factors when deciding whom to subject to surveillance.[63] These protections apply at the border.[64]

---

http://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/.

60 EFF, Digital Tips for Protesters (Nov. 16, 2016), https://www.eff.org/deeplinks/2016/11/digital-security-tips-for-protesters.

61 *United States v. Armstrong*, 517 U.S. 456, 464 (1996) ("the decision whether to prosecute may not be based on an unjustifiable standard such as race, religion, or other arbitrary classification"); *City of Cleburne v. Cleburne Living Ctr.*, 473 U.S. 432, 440 (1985) (laws that classify "by race, alienage, or national origin" are "subjected to strict scrutiny, and will be sustained only if they are suitably tailored to serve a compelling state interest"); *Obergefell v. Hodges*, 135 S. Ct. 2584 (2015) (striking down limits on same-sex marriage); *United States v. Virginia*, 518 U.S. 515 (1996) (striking down exclusion of women from state-run military academy).

62 *Church of LukumiBabalu Aye, Inc. v. City of Hialeah*, 508 U.S. 520 (1992) (striking down, under the Free Exercise Clause, a law targeting a religious practice); *Kiryas Joel Sch. Dist. v. Grumet*, 512 U.S. 687 (1994) (striking down, under the Establishment Clause, a law drawing public school district lines to match the neighborhood boundaries of a religious community). *See also Larson v. Valente*, 456 U.S. 228, 244 (1982) ("The clearest command of the Establishment Clause is that one religious denomination cannot be officially preferred over another").

63 *Hassan v. City of New York*, 804 F.3d 277 (3d Cir. 2016) (reversing dismissal of a lawsuit alleging that the NYPD violated the Equal Protection Clause, the Free Exercise Clause, and the Establishment Clause by targeting Muslims for surveillance).

64 While the U.S. Supreme Court did once suggest that border agents operating near the Mexican border could consider a traveler's ancestry (among other factors) to establish reasonable suspicion of an immigration violation sufficient to detain someone for questioning, *United States v. Brignoni-Ponce*, 422 U.S. 873, 886-87 (1975), that suggestion is no longer considered good law. Indeed, a U.S. appellate court held that this earlier ruling is not controlling in light of changes in constitutional law and population demographics. *United States v. Montero-Camargo,* 208 F.3d 1122, 1131-35 (9th Cir. 2000) (en banc). *See also* 8 U.S.C. § 1152(a)(1)(A) (prohibiting discrimination in immigration decisions on the basis of race, sex, nationality, place of birth, or place of residence).

Consent: Waiving Constitutional Rights at the Border

The constitutional protections described above can be waived. For example, the Fourth Amendment allows law enforcement officials to search people or their property if those people voluntarily consent to the search. [65]

That said, whether consent is truly "voluntary" depends on the totality of the circumstances, such as the nature of the questioning and the youth of the person being questioned.[66] There is a strong argument that a traveler's compliance when border agents demand the unlocking of a device, the device password, or social media information, should never be treated as voluntary consent. Border screening is an inherently coercive environment, where agents exercise extraordinary powers, and travelers are often confused, tired after international travel, and/or rushing to make a connecting flight.

However, courts may rule otherwise. It is possible that if you unlock your device, and agents then search your device, a court will rule that you consented to the search. It will depend upon the totality of the unique circumstances surrounding your particular border crossing.

As noted in Part 1, the best way to avoid an inadvertent "consent" to search is to decline to unlock your device, provide the device password, or provide any social media information.

What If You Are Not a U.S. Citizen?

EFF believes the U.S. government should respect the digital privacy of people from all nations. However, U.S. courts have held that foreign citizens arriving at the U.S. border enjoy fewer constitutional rights compared to U.S. citizens.

Foreign visitors have the fewest rights. For example, if a border agent refuses to allow them to enter the country, some may have no constitutional right to procedural due process (notice and a hearing) to challenge the exclusion.[67] Thus, if a foreign visitor refuses a border agent's demand to unlock their digital device, provide the device password, or provide social media information, and the agent responds by denying entry, the foreign visitor may have little legal recourse.

---

65 S*chneckloth v. Bustamonte*, 412 U.S. 218 (1973).

66 *Schneckloth v. Bustamonte*, 412 U.S. 218, 226 (1973).

67 *Landon v. Plasencia*, 459 U.S. 21, 32–34 (1982) (citing Knauff v. Shaughnessy, 338 U.S. 537, 542 (1950)).

Lawful permanent residents (LPRs or green card holders) enjoy more constitutional protection. For example, if LPRs are denied re-entry, they may have a constitutional right to procedural due process under the Fifth Amendment, depending on such factors as the duration of their trip.[68] However, the law regarding re-entry of LPRs is complicated, and it provides border agents discretion to consider many factors to challenge the continued status of residents.[69] If an LPR does not comply with an agent's demand to unlock a device, provide the device password, or provide social media information, that decision may negatively impact their re-entry processing.

Constitutional protections do apply if the U.S. government brings a criminal prosecution against a foreign citizen for smuggling contraband over the border.[70]

Foreign citizens should consult with a lawyer before they travel if they have questions about their legal rights at the U.S. border, including the ramifications of declining an agent's demand to unlock a device, provide a password, or provide social media information.

Also, to make it easier to communicate with a lawyer during a potential border detention, foreign citizens should complete a **Form G-28** before they travel.[71]

Federal Policies and Practices on Digital Searches

Federal Agencies That Oversee the Border

The U.S. Department of Homeland Security (DHS) is responsible for securing the nation from threats, including border security.[72] Its units include U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE).[73]

---

68 *Landon v. Plasencia*, 459 U.S. 21, 32–34 (1982) (citing *KwongHai Chew v. Colding,* 344 U.S. 590 (1953)). *See also Washington v. Trump,* 2017 WL 526497, *8 (9th Cir. Feb. 9, 2017) (procedural due process rights "apply to certain aliens attempting to reenter the United States after travelling abroad").

69 8 U.S.C. § 1101(a)(13)(C) (whether an LPR is treated at the border as an alien seeking admission depends, for example, on whether they abandoned their LPR status, and the duration of their absence from the United States); CBP, *International Travel as a Permanent Resident* (stating that abandonment of LPR status depends upon such factors as the amount of time spent abroad, the LPR's intentions, family and community ties, and location of employment, tax payment, and mailing address), https://www.uscis.gov/green-card/after-green-card-granted/international-travel-permanent-resident#travel.

70 *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985) (applying Fourth Amendment protections to a Columbian national detained at the border on suspicion of drug smuggling).

71 U.S. Citizenship and Immigration Services, G-28: *Notice of entry of appearance as attorney or accredited representative*, https://www.uscis.gov/g-28.

72 DHS, About DHS, https://www.dhs.gov/about-dhs.

73 DHS, *Dep't Organizational Chart,* https://www.dhs.gov/sites/default/files/publications/Department%20Org%20Chart_1.pdf.

CBP manages and controls the U.S. border, including customs, immigration, border security, and agricultural protection. On a typical day, it screens nearly one million visitors at the U.S. border.[74]

ICE investigates and enforces federal laws governing border control, customs, trade, and immigration.[75] ICE agents do not routinely search or interview travelers at the U.S. border. However, when CBP officers seize an electronic device at the border, they sometimes turn it over to ICE for further investigation.[76] ICE's Homeland Security Investigations (HSI) unit operates forensic laboratories that can process digital evidence.[77]

Device Search Policies

In 2009, CBP issued its agents a written directive on "Border Searches of Electronic Devices Containing Information."[78] It addresses search, seizure, and retention of digital information.

Search

- CBP claims authority to "examine electronic devices" and "review and analyze the information encountered"—"with or without individualized suspicion."[79]
- An officer may search an electronic device without supervisory approval if such approval is "not practicable," though notice to the supervisor is required afterwards.[80]
- When officers encounter information on an electronic device that may be protected by the attorney-client privilege, they must consult with the CBP legal office before searching it.[81] But this heightened review is no substitute for individualized suspicion, and cannot justify invasion of attorney-client confidentiality.
- When officers encounter "other possibly sensitive information, such as medical records and work-related information carried by journalists," they must follow

74 CBP, *About CBP*, https://www.cbp.gov/about.

75 ICE, *Who We Are,* https://www.ice.gov/about.

76 ICE, Border Searches of Electronic Devices, Directive No. 7-6.1, para. 6.2 (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

77 ICE, *Forensic Capabilities Strengthen ICE Investigations,* https://www.ice.gov/features/hsifl.

78 CBP, Border Search of Electronic Devices Containing Information, Directive No. 3340-049 (Aug. 20, 2009), https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.

79 *Id.* at para. 5.1.2.

80 *Id.* at para. 5.1.3.

81 I*d.* at para. 5.2.1.

"any applicable federal law and CBP policy."[82] It is unclear whether this provides any protection at all. It certainly is far less than individualized suspicion.

- If an officer searches an electronic device, they must complete an after-action report.[83]

Seizure

- Officers may detain electronic devices for *subsequent search* at an on-site or off-site location. If an officer does so, they must issue a custody receipt to the traveler (Form 6051D). The device detention should not exceed five days, though CBP managers may (and do) grant extensions of weeks or months.[84]
- Officers may *indefinitely* seize a device or retain copies of information on the device if, based on data uncovered during the initial search or other facts, there is probable cause to believe that the device contains evidence of a "crime that CBP is authorized to enforce."[85]
- If there is no probable cause, agents must return the device, and they must destroy any information copied, subject to the two broad and nebulous exceptions below.[86] This destruction must be documented.[87]
- CBP granted itself two substantial loopholes from this destruction rule. First, agents may retain information "relating to immigration, customs, or other enforcement matters" as allowed by various CBP record system rules.[88] Second, agents must "promptly share any terrorism information" with other federal agencies, which will manage and dispose of that information in accordance with their own rules.[89] It appears that the two exceptions swallow the rule.

The 2009 CBP policy empowers border agents to search devices, and authorized third parties to assist them, citing 19 U.S.C. § 507.[90] But authorization to search devices does not mean travelers must disclose passwords. The cited statute, empowers border agents to "demand the assistance of any person" to conduct a border search, and allows

82 *Id.* at para. 5.2.2.

83 I*d.* at para. 5.2.2.

84 *Id.* at paras.5.3.1, 5.3.1.1, and 5.3.1.4.

85 *Id.* at para. 5.4.1.1.

86 *Id.* at paras.5.3.1.2 and 5.3.3.4.

87 *Id.* at para. 5.3.1.2.

88 *Id.* at para. 5.4.1.2.

89 *Id.* at para. 5.4.1.4.

90 CBP, Border Search of Electronic Devices Containing Information Directive No. 3340-049, sec. 5.1.1 (Aug. 20, 2009), https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.

a $1,000 fine against a person who "without reasonable excuse" refuses such assistance.[91] But when Congress enacted this law in 1986, travelers were not carrying password-protected devices, so Congress could not have intended to address passwords. Even if it did, travelers have the ultimate "reasonable excuse": protection of their constitutional liberties. Most importantly, a statute cannot strip travelers of their constitutional liberties.

In 2009, ICE issued a similar policy.[92] It also authorizes searches and seizures "without individualized suspicion."[93] It sets a 30-day deadline for searches, though ICE managers may grant extensions.[94]

Searching Social Media and Other Cloud Content Without Using Travelers' Devices

Rather than use travelers' devices as portals to the cloud, border agents can demand that travelers disclose information about their online accounts: either their account identifiers or handles (which is now happening), or their account login credentials, that is, their usernames and passwords (which is now being proposed). Border agents can then use their own computers to find publicly available cloud content such as social media posts when they know identifiers/handles, and could access private posts and other private content by logging directly into online accounts.

In December 2016, the federal government took a big step in this direction. CBP now asks foreign citizens who enter the United States under the Visa Waiver Program (VWP) to voluntarily disclose their social media identifiers. The VWP enables citizens of dozens of participating countries to visit the U.S. for up to 90 days, without a visa, if they get approval from the Electronic System for Travel Authorization (ESTA).[95] Under the new CBP policy, ESTA presents VWP applicants with the following prompt: "Social media (optional) – Please enter information associated with your

91 19 U.S.C. § 507(a)(2).

92 ICE, Border Searches of Electronic Devices Directive No. 7-6.1 (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

93 *Id.* at para. 6.1.

94 *Id.* at para. 8.3.

95 U.S. State Dept., *Visa Waiver Program*, https://travel.state.gov/content/visas/en/visit/visa-waiver-program.html.

online presence."[96] Below this prompt are two fill-in boxes labeled "provider/platform" and "social media identifier."[97]

EFF and many other digital liberty organizations objected to this new policy.[98] Among other things, it invades the digital privacy of both foreigners and the U.S. citizens who communicate with them, and it may provoke other nations to impose the same burdens on U.S. citizens.

We also warned that this new policy is a major step towards mandatory disclosure (not just voluntary) of all private and public social media content (not just public) from all travelers (not just foreign citizens from VWP countries).

Our fears came true faster than we expected. In January 2017, the Council on American-Islamic Relations (CAIR) filed complaints with DHS alleging that border agents ordered U.S. citizens to disclose their social media information (as well as the passwords to their phones).[99]

As of this writing, government officials are also considering new policies that would further expand CBP scrutiny of travelers' cloud content, including *mandatory* disclosure of *private,* password-protected social media information.[100] These dangerous policies, if adopted, could easily be expanded to cover all travelers.

---

96 CBP, *ESTA application*, https://esta.cbp.dhs.gov/esta/application.html?execution=e1s1 . *See also 60-Day Notice and Request for Comments; Revisions of an Existing Collection of Information,* 81 Fed. Reg. 40892 (proposed June 23, 2016), https://www.federalregister.gov/documents/2016/06/23/2016-14848/agency-information-collection-activities-arrival-and-departure-record-forms-i-94-and-i-94w-and.

97 As of this writing, the Trump Administration is proposing a similar policy for Chinese visitors to the U.S. *See* Josh Gerstein, *Trump Proposes Including Chinese Visitors in Social Media Checks*, Politico (Feb. 17, 2017), http://www.politico.com/blogs/under-the-radar/2017/02/trump-chinese-visitors-social-media-check-235146.

98 *See, e.g.*, Letter from EFF to CBP (Aug. 22, 2016), https://www.eff.org/document/cbp-comments-final-aug-22-2016; Letter from Center for Democracy & Technology et al. (including EFF) to DHS (Aug. 22, 2016), https://cdt.org/insight/coalition-letter-opposing-dhs-social-media-collection-proposal/; Letter from Brennan Center for Justice et al. (including EFF) to DHS (Oct. 3, 2016), https://www.brennancenter.org/analysis/civil-liberties-coalition-submits-comments-dhs-plan-collect-social-media-information; Letter from David Kaye, U.N. Special Rapporteur, to Pamela K. Hamamoto, Ambassador of the U.S. to the U.N. (Sept. 30, 2016), http://www.ohchr.org/Documents/Issues/Opinion/Legislation/USA_9_2016.pdf. *See generally* Regulations.gov, Public Comments the *CBP*'s Information Collection Req't Concerning the Arrival and Departure Record, https://www.regulations.gov/docketBrowser?rpp=25&so=DESC&sb=commentDueDate&po=0&D=USCBP-2007-0102.

99 Press Release, CAIR Florida, *CAIR-FL files 10 complaints with CBP After the Agency Targeted and Questioned American-Muslims About Religious and Political Views* (Jan. 18, 2017), https://www.cairflorida.org/newsroom/press-releases/720-cair-fl-files-10-complaints-with-cbp-after-the-agency-targeted-and-questioned-american-muslims-about-religious-and-political-views.html. *See also* Sophia Cope, *Fear Materialized: Border Agents Demand Social Media Data From Americans* (Jan. 25, 2017), https://www.eff.org/deeplinks/2017/01/fear-materialized-border-agents-demand-social-media-data-americans.

PART 3: THE TECHNOLOGY OF PRIVACY PROTECTION

This primer on digital security technology provides a deeper dive into encryption and passwords, secure deletion, and cloud storage. Please note that while we discuss some specific services here, EFF does not endorse any particular technology or vendor.

Encryption

Encryption technologies can make stored information unintelligible to anyone who does not know the password. Encryption is especially valuable for portable devices because it reduces the chances of someone else getting access to your data without your knowledge if your device is seized, lost, or stolen.

Understanding Weaker Screen-Lock or User Account Passwords

Having to enter a password to use your device is not necessarily the same as having encryption. Many devices offer screen locks, for example, but nothing more. If you have a screen lock without encryption, an expert can bypass it in various ways and get access to your information without knowing the password.

We encourage you to ensure that your screen lock is set to the most protective setting available on each device. For example, protective options on phones, laptops, or tablets might include: locking automatically after a period of inactivity, locking the screen at start-up or requiring you to log in, always requiring a password to unlock, not allowing unlock with a fingerprint, and limiting the rate or number of attempted password guesses.

Having a screen-lock or user account password is a security benefit, and is much better than nothing if your device absolutely does not support encryption. But without encryption, experts will ultimately be able to bypass the password without your help.

100 *See* Sophia Cope, *Border Security Overreach Continues: DHS Wants Social Media Login Information* (Feb. 10, 2017), https://www.eff.org/deeplinks/2017/02/border-security-overreach-continues-dhs-wants-social-media-login-information

Strong Full-Disk Storage Encryption

The encryption technologies that are available to you will depend on your device and operating system. If it is available, the safest and easiest way to encrypt is to use built-in full-disk (full-device) encryption, as opposed to encrypting individual files or virtual folders on a device.[101] It is also possible that full-disk encryption was turned on automatically when you activated the device, as is the case for many recent smartphones. If that is true for your devices, you may still want to upgrade the strength of your password to maximize the security benefits.

As of this writing, built-in full-device encryption is available for the following systems:

- **Android**: some devices since Android 4.4 ("KitKat") [2013]; and all devices with Google apps since Android 6.0 ("Marshmallow") [2015].[102]
- **iOS**: encryption is available for all iPads; iPhone since 3GS or later; and iPod Touch since 3rd generation.[103]
- **Windows:** a built-in encryption tool, called "BitLocker," is available in some, but not all, editions of Windows since Vista [2007]; and device encryption in all editions since Windows 8.1 [2013].[104]

  Because forgetting encryption passwords is so common and the consequences are so severe, Microsoft chose in some versions of Windows to store a copy of users' decryption information with the company, so it can decrypt users' devices even if the users forget their passwords. If you do not want Microsoft to be able to decrypt your Windows device, you can opt out of this feature.[105] Windows

101 This is because software often leaves copies and references to files it is working with in unexpected places, where an expert could then easily discover unprotected information about the protected files. For example, a word processor may make unencrypted temporary copies of a document that was stored in an encrypted virtual folder, or an operating system may make unencrypted thumbnail copies of images, or any application may list names of encrypted files in a "Recent Documents" feature.

102 Since Marshmallow, all Google-licensed devices (which include Google apps) should include encryption and turn it on by default. Other Android devices should include an encryption option, unless the manufacturer has deliberately removed or disabled it, but may not have it turned on by default.

103 *See* https://ssd.eff.org/en/module/how-encrypt-your-iphone.

104 Microsoft sells each version of Windows in several "Editions." Some omit support for BitLocker. Since Windows 8.1, all editions have also included a "device encryption" feature, which is an alternative to BitLocker, and only works on supported hardware. Some versions of Windows also include the "Encrypted Filesystem" (EFS) feature.

105 *See* Micah Lee, *Recently Bought a Windows Computer? Microsoft Probably Has Your Encryption Key,* The Intercept (Dec. 28, 2015), https://theintercept.com/2015/12/28/recently-bought-a-windows-computer-microsoft-probably-has-your-encryption-key/. Depending on the Windows edition in question, you can either turn on device encryption without sending the recovery key to Microsoft, or log in to a Microsoft service to ask Microsoft to delete its copy of

users who do not have BitLocker or device encryption can choose to install third-party full-disk encryption software such as VeraCrypt.[106]

- **macOS:** a built-in encryption tool, called FileVault 2, has been available since MacOS X Lion [2011].[107]
- **Linux:** a built-in disk encryption system, called dm-crypt, has been in most distributions since the mid-2000s.[108]

More information on iPhone encryption can be found in EFF's Surveillance Self Defense guide: https://ssd.eff.org/en/module/how-encrypt-your-iphone

Activating Encryption

Activating encryption for the first time on your device can take a considerable amount of time because all of your data must be rewritten in encrypted form. It may take over an hour on some devices, so you may want to just let the process run overnight, with the device plugged in to AC power.

On most systems, if encryption is not already enabled,[109] you can do it yourself. You will be prompted to provide an encryption password. It may be different from the password you ordinarily use to log in or unlock the screen, and is sometimes only required when you power on the device. These details vary significantly from device to device. On some devices, such as iOS devices, your encryption password is *always the same* as your regular unlock password, and it is used both to unlock the screen and to decrypt the storage media.

Choosing a Strong Password

Strong passwords are critical for encryption. With some devices that do not use special hardware to limit password guesses, someone trying to crack your encryption can use a separate computer to try trillions of guesses very quickly. Such attacks can crack a word

---

your recovery key.

106 Wikipedia offers a comparison of disk encryption tools, both built-in and third-party. See Comparison of Disk Encryption Software, Wikipedia, https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software.

107 MacOS X versions since Panther [2003] included the original FileVault, which is not classified as full-disk encryption but should still be used if your device supports it.

108 On most Linux systems, full-disk encryption can only be enabled when you first install the operating system. If you have a Linux system without encryption, you'll generally need to reinstall the operating system to activate it.

109 For example, recent iOS devices are already using encryption even if you don't specifically ask them to. Thus, while you might want to upgrade your password, check your screen lock settings, and disable Touch ID, you don't need to do anything to turn on encryption on these devices.

or phrase that appears in a dictionary, or that could be predicted by some kind of rule (like changing certain letters into digits or punctuation marks), or any password shorter than about a dozen characters.

There are many ways to create long, unpredictable, yet memorable passwords. One approach is to choose a phrase made of several random words, which can be selected by a computer or by rolling dice. You may then be able to make up a mental story or mnemonic about these words to help you remember them. EFF has written our own guides to creating passwords using a version of Arnold Reinhold's "Diceware" technique, which you can find at:

- https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice
- https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases

There are other methods of making long, memorable passphrases, often based on sentences that you make up and then modify in some way. You should not use a phrase that has been published anywhere, such as a sentence in a book or song lyric. Computers can easily guess such phrases.

Encryption on iOS devices and some modes of Microsoft's BitLocker and device encryption use hardware features to ensure that your password cannot be guessed by using an external device capable of trillions of guesses (and, on some devices, limiting how often a password guess can be entered by hand). This could allow a shorter, simpler password to be secure in practice because an attacker can no longer try huge numbers of passwords quickly. However, we do not suggest relying on this because it can be hard to know what protections you get from the hardware and when.

Do Not Forget Your Password

A risk of encrypting your device is that nobody (including the device maker!) will be able to grant you access to your device if you forget your password. This is worth repeating because it is a very significant risk: **Forgetting your encryption password will permanently lock you out of the data on your device, and a technology specialist or manufacturer cannot bypass this**. This risk of losing access to your data makes it especially important to make regular backups.[110] If you do not use your encryption password regularly, you may want to write it down somewhere.[111] However, if you do

110 If you want, the backups can be encrypted too—but again, please be careful not to lock yourself out of every copy of your data by forgetting your passwords.

111 Password security advice has often suggested that you never write down a password, but a more recent consensus is that writing down passwords can be a good tradeoff to deal with the risk of forgetting them. A refinement to the old advice is not to write down your password *in the same*

not plan to unlock your device if border agents ask, you should not carry a copy of the password with you when crossing the border.

Turn Off Your Device

As we mentioned in Part 1, you should **turn off your device** before arriving at the border or any other risky situation. For a laptop, that means shut down, not just suspend or hibernate by closing the lid! This protects against several sophisticated attacks that could potentially extract the secret key or bypass the screen lock on a powered-on device.

Secure Deletion and Forensics

Many travelers may choose to delete things on their devices that they do not want others to see, or sensitive information that they know they will not need during their trips. This section discusses the possibility that data may not be permanently deleted, and some options for more thoroughly wiping devices.

Some "Deleted" Information Is Not Really Deleted

As noted in Part 1, there is a difference between what a border agent can glean from a casual inspection of your device (by tapping around or using the keyboard and mouse) and what can be determined by some forms of forensic examination. CBP and other law enforcement agencies have access to sophisticated forensic tools and experts. That means a forensic examination can, among other things, commonly recover deleted files and data and reconstruct information about how you have used your device in the past, even if that information is not apparent at all from a casual inspection. For example, forensic examinations routinely find deleted e-mails, files, and text messages, and also reveal the earlier presence and use of applications that have been uninstalled.

Many mobile devices also store information about how and when they were used. For example, mobile apps on a phone may have historic GPS information showing where you were at certain times in the past. A laptop or phone may have logs about when it was powered on, or the names of the wi-fi networks it has connected to. Sometimes, some kinds of activity log information are hidden from the user by default but can still be extracted and analyzed by a forensic expert.

If you want to feel more confident that your information has truly been deleted, read on.

---

place where the device it protects is kept.

Overview of Secure Deletion

There are tools that try to expunge information from storage media in ways that cannot be recovered by forensics. Most devices do not come with these tools. Their effectiveness varies widely, and it will usually be clear to a forensic examiner that they were used. We can refer to these tools as "secure deletion" or "wiping" software. Factory resetting your device may sometimes also fall in this category if appropriate encryption was used.

Note that border agents may notice, and regard as suspicious, a wipe or factory reset of your device, since most travelers do not routinely carry blank devices. Crossing the border with a blank device can be especially risky for non-citizens. Note also that truly secure deletion is irreversible and may be technically challenging for some travelers. Consider carefully whether you are comfortable deleting the information on your device. If possible, make sure you have made a backup copy of any important data before deletion, and leave that copy in a secure location.

Some secure deletion tools delete individual files, overwriting their contents so that they cannot be recovered. There are several things that can go wrong here: the most important is that references to the deleted files and their names may still exist, and so may temporary copies that software previously made while working with the files. It is safer, if possible, to delete an entire storage medium, although this may make a device unusable.

Secure deletion is easiest on laptops, and hardest on phones and tablets. It may be relatively achievable for digital cameras by taking out the memory card and wiping it in a laptop.

Built-in Factory Reset Features

Smartphones and tablets offer a "factory reset" feature that is designed to be used before you give or sell the device to another person.[112] These features are getting better over time in terms of the amount of data they remove. When used on an encrypted device, they may succeed in removing substantially all of the information from the device, although border agents could regard this as suspicious.

However, some models' factory reset operations may not actively overwrite the contents of the phone storage, so information could still be recoverable in a forensic examination. If you want to know for sure what information a factory reset will remove, you should consult the device manufacturer.

112 On Chromebooks, this feature is called "power wash."

Many devices have a removable memory card, like an SD card, which is used to store photos and other information. Factory reset often does not erase the removable memory card, so you should remove and wipe it separately, or swap it out for a new, blank memory card.

If your device offers an account-based cloud sync feature—such as iCloud—you may be able to sync your device before crossing the border, then factory reset it, then re-associate the device with your account and re-sync it after crossing the border. Make sure that the sync includes all of the data that you care about so that you do not lose anything important. However, keep in mind that re-syncing the device may take a long time and require downloading a lot of data, and thus require a reliable broadband Internet connection.

Wiping Hard Drives and Removable Media

A laptop can wipe its own hard drive, or removable storage media like USB drives or SD cards, by overwriting their contents.[113] One method of doing this is *formatting* the storage medium, but note that this term is applied to two very different processes: only "low-level formatting" (also called "secure formatting" or "formatting with overwriting") actually erases the hard drive by overwriting data, while "quick format" or "high-level format" does not do so. Formatting tools let you choose between a quick format and a secure overwriting format.

You should already have built-in tools that can already perform a low-level format or wipe a hard drive, or you may download third-party tools to do this. You should refer to the instructions for your operating system for securely wiping the hard drive.

After wiping a hard drive, you may need to reinstall the operating system before you can use the device again.

Again, this technique can be especially risky for non-citizens since it is highly unusual for travelers to carry blank devices with them.

113 In the past, security guides often suggested that it was necessary to overwrite multiple times (or "passes"). This may be true to some extent for flash media, as described below, but is apparently no longer true for traditional magnetic hard drives. *See* National Institute of Standards and Technology, *NIST Special Publication 800-88, Revision 1*, "Guidelines for Media Sanitization" (Dec. 2014) ("For storage devices containing *magnetic* media, a single overwrite pass with a fixed pattern such as binary zeroes typically hinders recovery of data even if state of the art laboratory techniques are applied to attempt to retrieve the data.").

Individual File Secure Deletion

For reasons noted above, trying to delete individual files, even using special secure deletion tools, may not produce the results you expect. Fragments of the files, or references to them, may still be present elsewhere on your system. Nonetheless, if you want to attempt this, we have described tools for this purpose in articles at:

- https://ssd.eff.org/en/module/how-delete-your-data-securely-linux
- https://ssd.eff.org/en/module/how-delete-your-data-securely-mac-os-x
- https://ssd.eff.org/en/module/how-delete-your-data-securely-windows

Clearing Free Space

If your operating system has a "clear free space" feature, you can use it to make it harder to recover deleted files. References to those files may still exist elsewhere on your computer, and it will be clear to a forensic examiner that you chose to clear the free space. Microsoft Windows includes a program called "Cipher" that can do this.[114] Third-party software like BleachBit is also available for this purpose. BleachBit can also be used to attempt to remove some individual programs' history, like web browser history, thumbnails, and recent document history, but we emphasize that this approach is imperfect.[115]

Flash Media

Some kinds of storage media based on flash memory technology have special issues[116] related to forensics and data recovery. These include SD cards, other memory cards used in cameras and mobile phones, USB flash drives, and some laptop solid-state drives (SSDs). If you are concerned about it, consider overwriting flash memory devices multiple times, not carrying them across the border, or consulting an expert on storage technology or computer forensics.

---

114 Typically, it's run with the command line CIPHER /W C:\ from a Windows command prompt.

115 *See* https://www.bleachbit.org/.

116 Because of a technology called w*ear leveling*, overwriting may not reliably delete these kinds of storage media in full. This technology tries to spread out where things are stored to prevent any one part of the storage medium from being used more than another part. Researchers have shown that even after the entire device has been overwritten, wear leveling may leave a small, random portion of the data on such media, and such data is recoverable. This forensic technique may require physically taking the storage medium itself apart, and does not appear to be in common use.

Encryption and Secure Deletion

Full-disk or full-device encryption can make secure deletion easier and more effective because wiping the only copy of the decryption keys should make the rest of the information on the device unreadable as a whole. This appears to be part of the functionality of a factory reset on iOS devices or a power wash on Chromebooks, which in turn means these devices can more easily and effectively be purged of their contents than other devices.

Whether or not a device has been wiped, full-device encryption can hinder or entirely prevent forensic analysis of its contents, if it is used correctly in accordance with other precautions, powering the device off, using a long and hard-to-guess passphrase, and not storing a copy of the passphrase somewhere where the examiner can later get a hold of it.

Cloud Storage

We are often reluctant to suggest storing data with online cloud services, because U.S. legal protections for cloud data can be less than the protection for data stored on your personal device. But in the border search context, the situation may be temporarily reversed: information that you have stored online may be more protected than information on a device you are carrying with you—because you are not carrying it across the border.

There are many options for storing information online, including several device makers' own cloud services. Some users may already be familiar with Microsoft OneDrive, Apple iCloud, and Google Drive, which are conveniently integrated with Windows, macOS, iOS, Android, and Chromebook devices. There are also many third-party options. Wikipedia offers comparisons of these services based on many factors:

- https://en.wikipedia.org/wiki/Comparison_of_online_backup_services
- https://en.wikipedia.org/wiki/Comparison_of_file_hosting_services

The Role of Cloud Storage in a Border Data Protection Strategy

Cloud storage is useful as a means to back up your data to prevent against data loss in case your device is seized, lost, or stolen. It can also be useful as part of a strategy for shifting data online so that it is not present on your computer while you are crossing the border.

It may also be feasible to store data online-only rather than keeping it on your computer at all. This is a default behavior for many purposes on Chromebooks, which is why many use them for travel.

Forensics

If you move data that was originally stored on your device to a cloud service, and attempt to delete that data from your device, you may not effectively delete it from your device. If your device is seized and subject to some forms of forensic examination, it may reveal some of the information that was previously stored.

Risks Associated with Cloud Storage

Cloud data is potentially accessible to governments (which can try to access it with a subpoena, warrant, or other legal process) and hackers (who can try to break into the cloud provider's systems). In the border search context you may—unusually—have stronger legal protections for data that is stored elsewhere, so it may be especially appealing to store some data online instead of on your device.

Most cloud services encrypt the data traveling between your computer and theirs, but then store it unencrypted, so they can read it and know what you are storing. A minority of cloud storage services, such as SpiderOak, offer *client-side encryption* where data is encrypted on your device before you upload it, so that the service cannot read the contents of your data. This is occasionally called "zero knowledge" in the industry. This is a great way to mitigate the risk that the storage provider will disclose your data to someone else. As with other applications of encryption, if you forget your password, the data will be permanently lost and no one can recover it.

The Wikipedia comparison charts above indicate whether or not data stored with each provider can be encrypted client-side before uploading.

Personal Cloud Storage

If you do not want to entrust your data to others in order to get the benefits of cloud storage, you can also host your own cloud storage with a server in a colocation facility, for example, using self-hosted cloud storage tools. As of this writing, one popular solution for this purpose is OwnCloud.

Some network-attached storage (NAS) appliances let you set up a password-protected web interface to upload, download, or synchronize files and folders over the Internet. If you have a fast, reliable broadband Internet connection at home and your Internet service provider does not block it, you could then have your own Internet-accessible

storage facility served from your own home. Some ISPs forbid home servers in their terms of service, so you may want to check to be sure.[117]

We strongly recommend using HTTPS encryption with either of these approaches to ensure network operators or other people on a wi-fi network cannot intercept your files and passwords.

Although a service that you host yourself offers a high degree of control and legal protection, it may be much more vulnerable to hacking compared to commercial cloud services because you will not benefit from a professional security team testing, monitoring, and upgrading it.

More Elaborate Data Minimization Ideas

Travelers with special needs or resources may be able to work out other approaches that reduce what they carry over the border. For example, an employer's IT department may be able to set up a cloud storage or backup system that limits access to some encrypted information under certain circumstances, or that installs a different version of an employee's computing environment for travel.

For personal travel, you may be able to physically remove the hard drive from your laptop before your trip, and purchase a separate laptop hard drive for travel purposes onto which you install a fresh operating system. Then you can swap hard drives before and after your trip and pick up where you left off when you get back home.

117 *See* https://www.eff.org/deeplinks/2013/08/google-fiber-continues-awful-isp-tradition-banning-servers .

CONCLUSION

We have fewer rights at the U.S. border than in the interior. Still, we can all take action before, during, and after our border crossings to protect our digital privacy. If border agents violated your digital privacy, please contact EFF. If you would like to help fight for stronger digital privacy protections at the U.S. border and everywhere else, please join EFF. Together, we can build a future where new technology strengthens our privacy and other constitutional rights, and does not diminish it.