Defending Privacy at the U.S. Border:

A Guide for Travelers Carrying Digital Devices

By Seth Schoen, Marcia Hofmann and Rowan Reynolds

Updated February 2012

ELECTRONIC FRONTIER FOUNDATION
eff.org

Table of Contents

Authors: Seth Schoen, Marcia Hofmann and Rowan Reynolds

Editing: Rainey Reitman and Mark Jaycox

Graphics and layout: Hugh D'Andrade

A publication of the **Electronic Frontier Foundation**, 2011

Copyright:
Defending Privacy at the U.S. Border: a Guide for Travelers Carrying Digital Devices is licensed under a Creative Commons Attribution 3.0 Unported License unless otherwise noted.

Defending Privacy at the U.S. Border:

A Guide for Travelers Carrying Digital Devices

Our lives are on our laptops – family photos, medical documents, banking information, details about what websites we visit, and so much more. Thanks to protections enshrined in the U.S. Constitution, the government generally can't snoop through your laptop for no reason. But those privacy protections don't safeguard travelers at the U.S. border, where the U.S. government can take an electronic device, search through all the files, and keep it for a while for further scrutiny – without any suspicion of wrongdoing whatsoever.

For doctors, lawyers, and many business professionals, these border searches can compromise the privacy of sensitive professional information, including trade secrets, attorney-client and doctor-patient communications, research and business strategies, some of which a traveler has legal and contractual obligations to protect. For the rest of us, searches that can reach our personal correspondence, health information, and financial records are reasonably viewed as an affront to privacy and dignity and inconsistent with the values of a free society.

Despite the lack of legal protections against the search itself, however, those concerned about the security and privacy of the information on their devices at the border can use technological measures in an effort to protect their data. They can also choose not to take private data across the border with them at all, and then use technical measures to retrieve it from abroad. As the explanations below demonstrate, some of these technical measures are simple to implement, while others are complex and require significant technical skill.

Why might people want to protect their data at the border?

- Business travelers, lawyers, doctors, or other professionals may have confidential or privileged information on their laptops that they don't want others to see or that they are obligated by law or contract to protect.
- People may have sensitive personal information on their devices such as medical records, financial documents, and years of correspondence with family, friends and business associates.
- Some travelers may have repeated difficulties crossing the border, and wish to take proactive steps to protect their data in light of their past experiences.
- Some may feel as a matter of principle that the government shouldn't be able to view their private information simply because they choose to travel internationally.

Why Can My Devices Be Searched at the Border?

The Fourth Amendment to the United States Constitution protects us against unreasonable government searches and seizures. This generally means the government has to show a court probable cause that a crime has been committed and get a warrant before it can search a location or item in which you have a reasonable expectation of privacy. But searches at places where people enter or leave the United States may be considered "reasonable" simply because they happen at the border or an international airport.

Several federal courts have considered whether the government needs any suspicion of criminal activity to search a traveler's laptop at the U.S. border. Unfortunately, so far they have decided that the answer is no.[1] Congress has also weighed several bills to protect travelers from suspicionless searches at the border, but none has yet passed.[2]

For now, a border agent has the legal authority to search your electronic devices at the border even if she has no reason to think that you've done anything wrong.

How the Government Searches Devices at the Border

There are two government agencies primarily responsible for inspecting travelers and items entering the United States: the Department of Homeland Security's Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). (Occasionally, CBP or ICE can make special arrangements to question a passenger departing from the United States or inspect her belongings, but neither agency routinely does so.)

The law gives CBP and ICE agents a great deal of discretion to inspect items coming into the country. While it's impossible to know for sure how they'll handle every border search situation, agencies have published their policies for searching electronic devices and data.

CBP tells its agents that "with or without individualized suspicion," they can inspect electronic devices and data encountered at the border.[3] The agency can keep your computer or copies of your data for a "brief, reasonable" amount of time to be searched on- or off-site. Ordinarily, this isn't more than five days.[4] CBP recognizes that agents might run across privileged or sensitive information stored on devices, but does not clearly explain the procedures for handling it.[5] When CBP agents experience technical difficulties or encounter information that is encrypted or written in a foreign language, they may send the device or a copy of the data to other government agencies that might be able to help access the information.[6] Border agents don't need any suspicion of wrongdoing to seek this assistance,[7] and it's unclear whether the cooperating agencies can keep copies of the data they receive indefinitely.

Which Three-Letter Acronym Was That Again?

The **Department of Homeland Security (DHS)** has several departmental missions, including to "secure[] the nation's air, land and sea borders to prevent illegal activity while facilitating lawful travel and trade." Department of Homeland Security Missions and Responsibilities, http://www.dhs.gov/xabout/responsibilities.shtm (last visited Oct. 4, 2011).

Customs and Border Protection (CBP) is the primary agency that inspects and searches travelers entering the United States. For example, when you arrive in the U.S., you can expect to be interviewed at the border by a CBP agent and to present your Customs declaration to another CBP agent.

Immigration and Customs Enforcement (ICE) investigates violations of laws related to borders. Although ICE has border search authority, it isn't routinely involved in searching or interviewing travelers at ports of entry.

The **Transportation Security Administration (TSA)** is responsible for transportation security within the United States, and does not perform searches at the border. Normally, TSA searches travelers before they board a plane, not after they land. You can expect to be searched by TSA when departing the U.S. by air, but the screening TSA performs is usually identical for domestic and international passengers.

Like CBP agents, ICE agents may inspect electronic devices and the information on them "with or without individualized suspicion."[8] ICE will typically complete searches of devices and copies of data within 30 days,[9] though anecdotal reports suggest that travelers' devices are sometimes detained for significantly longer periods of time.[10] ICE's policy, like CBP's directive, says that agents may seek technical assistance from others to translate or decrypt data,[11] and is similarly vague about how agents should handle privileged or sensitive information.[12]

Beyond seizing the device at the border, the government may take a device to a location away from the border for further inspection.[13] If this occurs, searches of devices that are conducted at a time and/or place removed from the initial border stop can become extended border searches that require reasonable suspicion of wrongdoing or even regular searches that require a probable cause warrant.[14]

In short, border agents have a lot of latitude to search electronic devices at the border or take them elsewhere for further inspection for a short period of time, whether or not they suspect a traveler has done anything wrong.

For now, the government searches only a small percentage of international travelers' electronic devices. According to documents obtained by the American Civil Liberties Union through the Freedom of Information Act, more than 6,500 people traveling to and from the United States had their electronic devices searched at the border between October 2008 and June 2010, an average of more than 300 border searches of electronic devices a month. Almost half of those travelers were U.S. citizens.[15] This means that these searches are a regular occurrence, but one that most travelers will never encounter given the number of travelers who cross the border each month.

The frequency of technology-oriented searches at the border may increase in the future. Researchers and vendors are creating tools to make forensic analysis faster and more effective, and, over time, forensic analysis will require less skill and training.[16] Law enforcement agencies may be tempted to use these tools more often and in more circumstances as their use becomes easier.

Deciding How to Protect Your Data

Different people will choose different kinds of precautions to protect their data at the border based on their experience, perception of risk, and other factors. **There is no particular approach we can recommend for all travelers.** These are some of the considerations you might take into account:

- **Your citizenship, immigration, or residence status.** If you are not a U.S. citizen, you may be more easily denied entry into the country, and so you may want to be especially careful to avoid situations where border agents might consider you uncooperative for taking steps to protect your data or politely refusing to provide encryption passwords.

- **Time sensitivities.** Is it important for you to reach your destination by a certain time? If border agents hold you up with questioning or attempts to search your devices, it may wreak havoc on your travel schedule.

- **How much hassle you're willing to tolerate from border agents.** If you want to secure your data but are uncomfortable about the possibly of appearing uncooperative with border agents, it might be best to avoid such awkward situations all together. For example, you might choose to take a blank device over the border and download your data once you reach your destination rather than face an uncomfortable interaction with a border agent who wants to search the data on your device.

- **How important it is for you to have access to your data during your journey.** Consider whether you'll need your data with you on the plane, or whether you can wait until you've crossed the border to access it.
- **How good your Internet access will be during your travels.** If you'll have access to lots of bandwidth, you might be able to download the data you need once you reach your destination.
- **The countries you've visited before entering the United States.** Travel to certain countries may draw additional scrutiny from border agents.
- **Your history with law enforcement.** If you are subject to an ongoing investigation or otherwise under suspicion for any reason, you may be screened or questioned more intensively.

Case Scenario: Business Concerns

Alice is a frequent business traveler who often needs access to proprietary information that her company considers highly sensitive and confidential. When she travels for work, she takes a special laptop that contains the minimum information necessary for her trip. Before she leaves the country, she uses strong cryptography to encrypt that information. She also sets up two separate log-in accounts on the computer: a protected account where the encrypted files may be accessed, and a separate account for other uses of the laptop. Anyone who wants to view the confidential data must log in to the protected account and then decrypt the files. Only Alice's employer knows the passwords to the account and encrypted data, and the company's IT department sends the passwords to her in an encrypted email message so that she can access the data abroad. Before she returns to the U.S., she securely wipes her laptop.

Some Basic Precautions

All computer users who carry important information on portable devices should be aware of two basic precautions:

- Making regular backups, which ensures that your important information stays available to you if your computer is ever taken from you, lost, or destroyed. (If you don't have access to your computer, you'll still have access to your data.)
- Encrypting the information on the computer, which ensures that your information stays confidential from other people whom you don't authorize to access it. (If you lose control of your computer, other people won't have access to your data.)

In the infancy of personal computing, experts put particular emphasis on the need to make backups. Today, we think these two precautions are really halves of a larger whole: making sure that that information stays available to those you want to have it, and that it's not available to others. Applying these precautions can help you deal with travel incidents well beyond the comparatively unusual case of border searches, like if you leave a laptop in a taxi or if someone steals your backpack or purse from a café.

The right time to get started with both of these precautions is before your trip, when you're at home or at work and have more time and greater access to other people who can help you get set up appropriately.

There are also other more elaborate precautions which you might find useful. After discussing the basics, we'll suggest several of these below. Note that many of the precautions we will discuss address the possibility that your electronic devices are taken away from you, and examined for hours by a trained expert. For travelers who feel that this is an important concern, it's worth understanding what the capabilities of that expert examiner may be.

Backups

Every year millions of computer users lose important information accidentally for want of a good, current backup, so there are many good reasons other than the possibility of a border search or seizure for you to have a current backup. In modern practice, backups are most often made onto another computer over a network. (See our discussion of on-line service privacy in the next section – *Backups Using the Internet*.) You can also back up to an external hard drive, which can be extremely quick and easy.

Backups are especially important for travelers, since, aside from the possibility of a border search or seizure, travel presents many opportunities for losing your computer or data.

Backups Using the Internet

When you're backing up your computer over a network, bear in mind that

- Your **connection to the server** should be encrypted to prevent eavesdropping that would reveal the contents of your backup.
- The **content of your backups** should also be encrypted so that the backup service itself can't read them. (Currently, only a few services automate this process for you.)
- Your backups should be frequent, especially while you're traveling away from home. They can be **incremental** so that only things that have changed since your previous backup are actually transmitted over the network.
- Your Internet access will need to be **fast enough** to transfer the amount of information you have to back up in the time you have available.

Storing information with an online service, sometimes also called a "cloud service," is a popular choice today; it may have significant benefits for reducing the amount of data that could be exposed to a border search. For instance, you could keep your email with a webmail provider and not on your laptop, or edit documents on a network service like Google Docs, or store files with a service like SpiderOak instead of on your computer. Devices like Chromebooks can do this automatically so that you rarely physically store information on a laptop at all. Relying on network services and network storage has both advantages and disadvantages for privacy.

Pro: Data is not stored on your device, is not actually carried across the border, and is not subject to a physical border search. You can truthfully tell agents that the data is simply not present on your device at all; you are not carrying it with you.

Con: Some data that you store with a third-party online service provider in the United States enjoys less legal protection than data you store on your own computer.

You can get the best of both worlds when you encrypt your data separately before storing it with a cloud storage provider. Then the cloud storage provider does not know the information required to decrypt the data, so it can't access your data at all. Some cloud storage providers like SpiderOak[17], Tarsnap[18], and Wuala[19] make this kind of protection a standard part of their services, while tools like Duplicity[20] and Tahoe-LAFS[21] let you set up your own encrypted backup infrastructure.

If you decide to move some files into cloud storage before crossing the border rather than keeping your files there all along, remember that merely deleting files won't always remove their names or contents from your device. See The Challenges of Secure Deletion, below.

Hard Drive Image Backups

If you have a large external hard drive at home, you can make a byte-for-byte image copy of your laptop hard drive before your trip; then you can install a fresh operating system for travel purposes, overwriting the laptop contents. When you return home, you can restore the image copy onto your laptop (overwriting the travel operating system) and pick up where you left off.

Regardless of what operating system you usually run, you can do this most easily with a Linux live CD. (This operation happens below the level of the operating system, so it can be used on any operating system.) The external drive to which you make the backup should itself be encrypted, because the backup contains all of the information from your hard drive (including things you may think are deleted, and including saved passwords and authorization credentials) in a usable, accessible form.

Note that making or restoring a full-drive backup can take a long time; it's usually limited by the capacity of the connection to the external hard drive and could be up to several hours for a large laptop drive.

Since hard drive sizes have been growing faster than Internet connection speeds, image backups over the Internet are unlikely to be feasible except in the most highly Internet-connected places. (An Internet-based image backup is similar to swapping hard drive images onto an external disk, except that the external disk isn't physically plugged into the local computer but is located somewhere else. Encryption should be used to protect the hard drive's contents.)

Backups Using an External Hard Drive

You can also easily make a backup onto an **external hard drive** instead of (or in addition to) a network server. This hard drive can, and should, be encrypted so that only someone who knows the proper passphrase can read its contents. In general, store and transport your backup and your computer separately. In particular, **we recommend you don't carry your backup across the border at the same time as the computer it's backing up!**

Remember that backups can take time, so plan accordingly. Using a USB connection, a 60 GB laptop drive could take over 15 minutes to back up (probably longer), while a 1 TB drive could take around five hours. You can use incremental backups together with encryption to make the time a bit shorter. USB's peak data rate is 60 MB/s (for USB 2, the latest version you can assume is widely supported), so plan ahead and use incremental backups where appropriate. Note that current computers might let you connect external drives using Firewire, or eSATA interfaces as well, although the most universally compatible is USB, which is also the slowest (unless you have USB 3, which is still uncommon as of mid-2011).

A 2 TB external drive (self-contained and ready to use) is relatively cheap and is probably more than sufficient for a complete encrypted backup of any computer you're likely to use. You can also get an **enclosure** to turn an internal hard drive into an external hard drive. High-quality enclosures are also relatively inexpensive and protect the internal drive against physical damage, as well as providing power and making it easy to plug and unplug the drive.

Case Scenario: Doctor Confidentiality

Akina is a doctor in Japan. She is traveling to the United States with her young son to attend a relative's wedding. She wants to ensure that she can access any email messages that her patients send her while she is abroad, and considers it critical to protect the confidentiality of those messages. On the other hand, she doesn't want any confrontation with the border agents — she worries that being detained will upset her child, and, if they are refused entry, they will miss the wedding. Akina chooses not to carry a laptop at all. Instead, before her trip, she mails a travel laptop to her relative in the United States. After the wedding, she securely wipes the laptop and takes it back to Japan with her.

Minimizing Data You Carry

One strategy for protecting your data when traveling is to minimize how much data you carry. This can be as simple as choosing not to bring a device which may hold sensitive data with you during a border crossing, or it can involve removing data you don't want border agents to access. There are a wide variety of ways to effectively remove data, depending on the devices and network access that you have.

One approach is to **physically remove the hard drive from your laptop** before your trip. You might purchase a **separate laptop hard drive for travel purposes** and install a fresh operating system on it. Then you can switch hard drives before and after your trip and pick up where you left off when you get back home.

Alternatively, you can remove your hard drive before your trip and **use your computer with no hard drive at all** (by starting an operating system from a CD, USB drive, or SD card). See the Operating System on an SD Card section below for a more detailed discussion. Instead of storing files on a hard drive, you can store them on a USB or SD medium or on a network server that you access via an encrypted connection. Again, in this scenario, you can put your normal laptop hard drive back in when your trip is complete. In any case, you can ensure that the information on your laptop while you're traveling is minimized and that you have only the information you'll need during the trip.

Case Scenario: Philosophical Grounds

Howard firmly believes as a matter of principle that the government has no business sifting through the contents of his laptop, and he's willing to stand up for that belief. He is entering the United States after traveling around Asia for three months. He backs up his data on a remote server before his trip. He also uses strong cryptography to encrypt his hard drive and chooses a strong passphrase. If the border agents ask him for the passphrase, he intends to say no. He knows this might cause the agents to seize the laptop, but they are unlikely to break the password, and he can still have access to the information on the laptop because he has stored it remotely.

You could also use an **inexpensive travel computer** on which, by design or by practice, you avoid saving files, instead storing them "in the cloud" on network servers. A traditional netbook is suitable for this, while a Chromebook running ChromeOS helps automate the process. (Bear in mind that common application software could leave forensically recoverable data on the local hard drive even if you normally only save files on network servers.) They could make good investments for frequent travelers. Note that, if you do consider using cloud data storage, it's important to keep in mind the privacy concerns associated with giving a service provider access to your data; for instance, though Chromebooks store little data locally, Google can access the information these devices store in Google's cloud service. We discuss these issues in Backups Using the Internet, above.

As a way of limiting what they physically carry across an international border, some travelers will **send computers, hard drives, USB flash drives, or SD cards through the mail or other shipping service.** The legal protection afforded to computers and data sent via international mail is not appreciably better than at border crossings,[22] but travelers can at least know that they won't be questioned about those devices while they and the devices are both under border agents' control.

Thinking carefully about risks to portable devices and the data they carry is important for any traveler, not just those who will be entering the United States. The New York Times reported that "officials at American government agencies, research groups and companies that do business in China and Russia" carefully limit data they carry on laptops and mobile phones into those countries because of a perception that sophisticated electronic espionage techniques may be practiced against their devices.[23] The Times quoted U.S. Rep. Mike Rogers as preferring to be "electronically naked" when visiting China; the paper added that travelers who believe they are likely targets of espionage fear not only that data will be copied, but also that hardware or software bugs may be surreptitiously installed on their devices.[24]

The Challenges of Secure Deletion

Simply deleting data from your hard drive with your normal OS file deletion features is not secure and the data is still present and recoverable on your hard drive. Just because deleted files are no longer visible in your operating system's file manager does not mean that a forensic expert can't undelete them or deduce that they were once present. The forensic software will examine the bytes actually stored on disk, which contain much more information than your operating system shows you.

Even if you delete files securely when uploading them, there might still be local traces of those files' contents because of cached copies, metadata, and swap space issues.[25] For example, file names of cloud-stored files may still be mentioned on your hard drive. Perhaps copies of some of them are temporarily downloaded while you're working on them, and the local traces or even the complete contents would then be visible with appropriate forensic software.

Securely erasing files requires overwriting them, not just pressing "delete" in the user interface or emptying an electronic wastebasket. As Simson Garfinkel explains, it also doesn't work to just "format" a hard drive on most systems.[26] Remember: an action may appear to erase or sanitize data, but may be easily undone by a knowledgeable forensic examiner.[27]

You can use DBAN[28] to delete entire laptop hard drives (or external hard drives or memory cards) safely. According to more recent research, multiple-pass overwriting (something extensively promoted during the 2000s) is probably not necessary. This is important because multiple-pass overwriting often takes most of a full day and has discouraged people from using secure deletion tools, especially if they're in a hurry. Single-pass overwriting in a correctly-implemented secure deletion tool is qualitatively much better than nothing, and especially much better than deciding not to overwrite data at all because of the time it would take!

There are some types of software — known as secure file deletion utilities or Secure Empty Trash — which might be be useful for erasing individual files safely. However, in modern computing environments, these methods are not necessarily fail-safe when faced with expert forensic analysis. We do not recommend that you rely on them for removing your sensitive data from a device.

Some operating systems have a useful way to "clear free space" on a disk. If your system has this feature, it helps make most kinds of deleted data hard to undelete, but deleted regions or data within files or databases may not be purged if the files or databases themselves still exist. For example, clearing free space should prevent the undeletion of deleted files, but perhaps not undeletion of deleted emails and web history if they were stored inside of larger files that still exist.

A perennial problem is that many kinds of application software invisibly leave traces behind when you open or work with files. For example, applications might make a temporary copy, or list a file's name in a "Recently used documents" list. Forensic software is written to be aware of these traces and search them out. This is also a substantial risk for people who use disk encryption to protect data on removable storage devices.[29] With this concern in mind, the most prudent course would be to assume that some trace of any files viewed or edited on a particular computer could still be present on that computer's hard drive. That's why using full-disk encryption is, according to some researchers, "the safest strategy" (although less helpful if you anticipate turning over your passphrase if asked).

Operating System on an SD Card

On the most modern laptops, it's possible to use an SD card like a hard drive; thus, you can choose to use an SD card in place of a conventional hard drive and keep your entire operating system and all your data on on it. (You should still use disk encryption for the data on the SD card.) Since you can keep the SD card in your pocket or wallet when it's not in use, it's considerably harder for someone to take it from you without your knowledge or tamper with it (although, since it's so tiny, it's much easier to lose).

You can also easily prepare several different operating system images on separate SD cards, for separate purposes or separate trips. In this case, it's easier to send them in the mail or even easily erase or destroy a card when you no longer need it. Privacy expert Chris Soghoian, who described this technique, reports that his laptop gets better battery life when he uses an SD card in place of a hard drive[30].

You can even use the same SD card in a digital camera for taking photos, so that a single card serves both as your camera storage medium and your encrypted hard drive.

Encryption

Disk encryption protects your data if your computer is ever lost or stolen during your travels, so it's a useful precaution even for people who plan to cooperate completely with border agents' requests for assistance in inspecting devices. Also, using encryption can help ensure you know whether your computer was actually searched, because you are "in the loop" — a successful search will not happen without your knowledge. If you don't use full-disk encryption, border agents can search your computer in another room and you won't necessarily know whether this has happened, because they will not require your cooperation.

Threats to Disk Encryption

Full-disk encryption is not an impregnable solution to all concerns about data privacy. It could conceivably be bypassed in certain ways:

- By breaking into your computer while you're using it (with a Trojan horse or *spearphishing*, or exploiting a vulnerability in software that you use).
- With a ***cold boot attack*** if the attacker has control of your computer while it's turned on, after you've already entered your passphrase (even if the screen is locked or the computer is in "suspend" mode).
- With an ***evil maid attack*** if the attacker has control of your computer while it's turned off and you use it later on without realizing the attack has happened.
- By learning your encryption passphrase or key with high-tech surveillance techniques (such as video surveillance or emanations monitoring).

A simple precaution against cold boot attacks at the border is available. **You should always turn off your computer (physically power off, not "suspend" or "hibernate", and not just closing the lid) before crossing the border.** If a computer is on and you have previously entered the disk encryption passphrase, there are techniques for extracting it directly from the computer's memory (even if the screen is locked). Powering the computer off prevents these techniques from working.

Account Passwords Versus Full-Disk Encryption

People often decide that they need to "set a password on their computer" in order to protect their data. This intuition is right, but the details matter quite a lot; not all ways of "setting a password" provide the same kind of protection, and many don't involve any encrypton.

An **account password** or **screen-lock password** is enforced by the operating system code. The operating system is configured to ask for the password and won't allow access unless the right one is provided. But the data is still simply present on the hard drive. An account password is easily bypassed by accessing the same disk using a different operating system, which won't require that the correct account password be entered. Alternatively, the hard drive could be physically removed from the computer and read using a different computer; again, no password would be needed.

By contrast, **disk encryption** uses mathematical techniques to scramble data so it is unintelligible without the right key. This mathematical protection works independently of the policies configured in the operating system software. A different operating system or computer cannot just decide to allow access, because *no computer or software* can make any sense of the data without access to the right key.

This distinction makes a major practical difference. Bypassing an account password is a routine operation that can be done automatically with forensic software that bypasses the operating system and looks directly at the disk, interpreting its contents for the forensic analyst; your account password is no obstacle for this forensic software. CBP, ICE and other federal law enforcement agencies have staff with extensive training in the use of forensic software and are prepared to use it if they think the contents of your computer are interesting enough.

Fortunately, modern computer systems come with comparatively easy full-disk encryption tools that let you encrypt the contents of your hard drive with a passphrase that will be required when you start your computer. *Using these tools is the most fundamental security precaution for computer users who have confidential information on their hard drives and are concerned about losing control over their computers — not just at a border crossing, but at any moment during a trip when a computer could be lost or stolen.*

Case Scenario: Documentary Filmmaker

Bill is a filmmaker who has made several documentaries over the past few years about the efforts of authoritarian governments to suppress dissent in their nations. He traveled to a couple of Middle Eastern countries last year, and has faced heavy questioning at the U.S. border ever since. He is working on a new project in Tunisia, where he filmed interviews with several dissidents, and he wants to do everything possible to protect the confidentiality of this footage. He needs to transport several hundred GBs of video into the United States from Tunisia. His Internet access is not good, so uploading it to a remote server is not a realistic option. Bill chooses to store the encrypted video files on discs with a strong passphrase and asks a friend to mail them to him in the United States. Then he securely wipes his laptop and brings it back into the United States with him.

Choosing a Disk Encryption Tool

Choosing encryption tools is sometimes challenging because there are so many options available. For the best security, choose a **full-disk encryption** tool that encrypts everything on your computer rather than a **file-encryption** tool that encrypts individual files separately. This may need to be set up at the time your operating system is first installed. Every major operating system now comes with encryption options.

- Microsoft BitLocker in its most secure mode is the gold standard because it protects against more attack modes than other software. Unfortunately, Microsoft has only made it available with certain versions of Microsoft Windows.
- TrueCrypt has the most cross-platform compatibility.
- Mac OS X and most Linux distributions have their own full-disk encryption software built in.

For more detailed information about the advantages and disadvantages of various tools, consult the Wikipedia article on comparison of full-disk encryption software.[31]

Choosing a Secure Passphrase

Unlike other passwords, cryptographic passwords specifically need to be **long and extremely hard to guess.** This is because a computer (or a cluster of many computers) can be programmed to try trillions or quadrillions or more of possibilities automatically. If the password is too short or otherwise constructed in too predictable a way, this **brute force** guessing approach will eventually succeed in cracking the password by trying every possibility.

Approaches to choosing encryption passwords that don't take account of this reality are obsolete. For instance, many users have historically been trained to use random passwords around 7-8 characters and containing letters, numbers, and punctuation marks, like these:

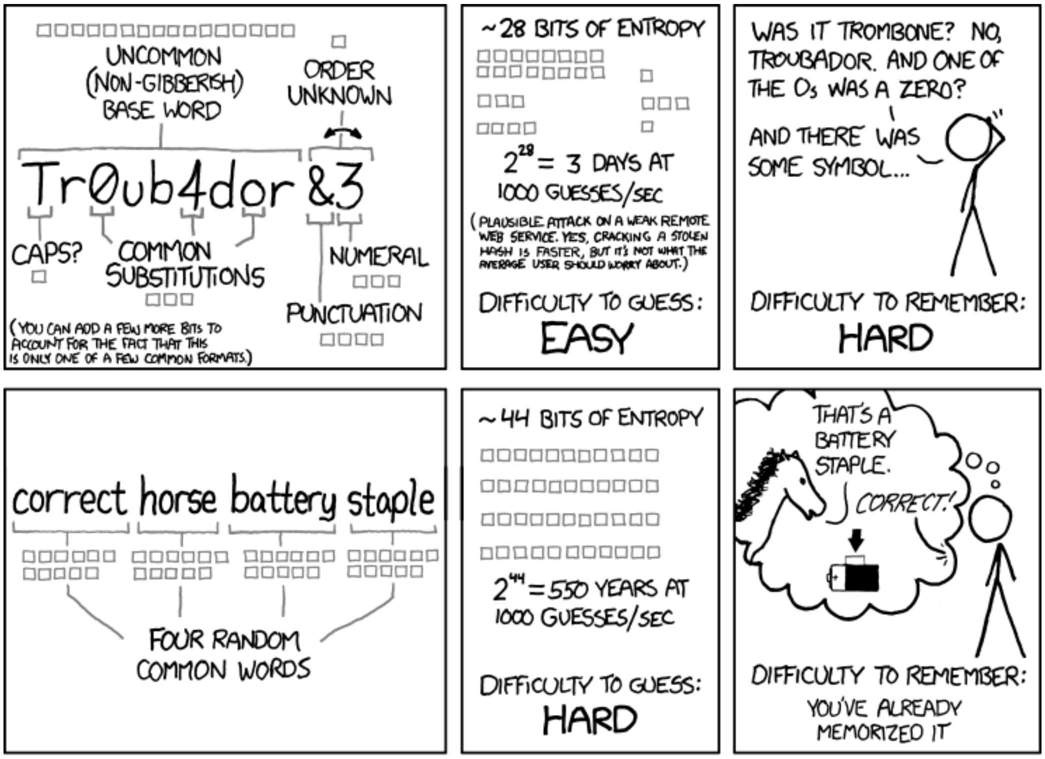
1rThlr'9 &&0HfxEV iq#tW}i7 9/NKgKal G>oX/7Ip s@;30:[E

These passwords are certainly hard to remember and hard for a human being to guess, but they're *simply not safe enough as cryptographic passwords* against modern crypto-cracking devices, which would easily be able to guess each of them. In 1999, EFF built a crypto-cracking machine that could try 2^{56} possibilities in under nine days.[32] That's about enough to try *every nine-letter password* made of letters, numbers, and punctuation. Bear in mind that this was a non-profit organization's proof-of-concept project from twelve years ago! It's a certainty that government agencies can crack even longer passwords with ease today.

Fortunately, modern practice provides useful alternatives. Instead of using a single word as an encryption password, it's now normal to use a long text called a **passphrase**.[33] Arnoud Engelfriet defines a passphrase this way:

> A passphrase is a sentence or phrase used instead of a single password. Because of its length, a passphrase is more secure than a password. By using a phrase, it still is easy to remember.[34]

While some traditional advice emphasizes (correctly) that one should not use a dictionary word *as* one's password, modern practice shows that using multiple dictionary words *in* one's passphrase is useful. Our calculations confirm that relatively short series of truly randomly chosen English dictionary words are secure; many people find these somewhat more memorable. The important thing is to choose *enough* words and to choose them *in a random way*. A useful technique for choosing secure passphrases with combinations of words is called **Diceware**; this approach was devised by Arnold G. Reinhold.[35] The Diceware approach can be carried out with actual physical dice, or using any of a variety of software applications, and offers a complete recipe for making safe and memorable passphrases.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

A major advantage of passphrases made of words is that it's often possible to think of a mnemonic that allows you to easily memorize your passphrase. Randall Munroe's xkcd comic shows a typical example for the Diceware-like phrase "correct horse battery staple"[36]: a horse is being congratulated on correctly identifying a staple protruding from a battery.

Note: this phrase, while memorable, is likely not long enough to be truly secure against cracking by specialized encryption-cracking tools or machines, since Munroe's advice doesn't aim to protect against this kind of attack. A strong passphrase would be longer or incorporate words from a larger word list, usually resulting in something more like: "exultantly barnacle slipshod Vancouver rumble." This is also memorable! The Diceware article discusses in more detail how to ensure your passphrase is long enough.

Another popular modern approach is to use a phrase, sentence, song lyric, poem, or long acronym *that has been modified in an unguessable way*, such as by changing the spacing, punctuation, spelling, or capitalization in an idiosyncratic way, or altering the topic of the text or combining several unrelated texts together.[37]

When encryption passphrases are forgotten, the disk contents will become completely unusable. By design, the disk encryption software author is unable to override or bypass the protection. Some systems like BitLocker suggest making a spare copy of the passphrase and storing it somewhere safe and inconspicuous, physically distant from the computer it protects. There are also technologies for allowing multiple people to share parts of the passphrase so that it can only be recovered if several of them cooperate (usually, implementations of Shamir's Secret Sharing Scheme, such as the ssss[38] and Secret Sharp[39] software). If you worry that you might forget your passphrase, you could use this software to securely split it into pieces and store the pieces in different places.

TrueCrypt Hidden Volumes

The TrueCrypt encryption software tries to provide "deniability" by letting you create multiple encrypted disks protected by separate passwords in such a way that the ***existence*** of additional hidden data can't be easily proven or disproven. These additional encrypted disks are known as **hidden volumes**. Although TrueCrypt hidden volumes may have some practical applications, we think they are **unlikely to be useful in the border search context** because they are most helpful when lying to someone about whether there is additional hidden data on a disk. Lying to border agents is not advisable, because it can be a serious crime.

Border Agent Demands for Access to Data

If a border agent asks you to provide an account password or encryption passphrase or to decrypt data stored on your device, you don't have to comply. Only a judge can force you to reveal information to the government, and only to the extent that you do not have a valid Fifth Amendment right against self-incrimination.[40]

However, if you refuse to provide information or assistance upon request, the border agent may seize your device for further inspection or consider you uncooperative, which the agent may take into consideration when deciding whether to allow you to enter the United States.

If you are planning to bring encrypted or password-protected information over the border, it's best to decide ahead of time how you would respond to a border agent's request for help to inspect data. The best answer for your particular circumstance may be to cooperate or to politely decline to provide information. You could also choose to avoid the situation altogether by bringing a blank device over the border and downloading your data once you reach your destination.

Another option is to generate a long and not-very-memorable encryption password before your trip, and then have someone else hold onto it and send it to you later, after you've crossed the border. This might be especially practical with a work computer if you have support from an IT department at your workplace, because the IT department could hold onto the password for you and let you know it when you check in with them again.[41]

For more advice on dealing with agents at the border, see the section titled *Interacting with Border Agents*.

Technology-specific Considerations

Flash Drives

Flash memory devices (including USB flash drives and SD cards) are used as the internal storage in most cell phones and digital cameras. Securely erasing their contents can pose an extra challenge because of a technology called wear leveling, which tries to prevent you from repeatedly writing to the same place on the disk. That means that special forensic techniques involving physically disassembling the flash drive can sometimes reconstruct contents that you attempted to overwrite, because the flash drive decided to put the overwriting data in a different physical location from the overwritten data.[42] This kind of forensic examination is much rarer than basic disk forensics and is probably only a concern in a tiny number of situations.

Mobile Phones and Similar Devices

Devices like mobile phones increasingly hold tremendous amount of sensitive information, including photos and email messages that just a few years ago might have been found only in cameras and laptops. Often, they contain lists of your friends and colleagues and detailed logs of when you communicated with them. Some mobile phones also store detailed logs of your physical location over time.

Although setting a password on your phone can be a sensible precaution, it's worth emphasizing that the password and screen-locking features that come with most phones provide no meaningful protection against a skilled examiner. These passwords are like user account passwords on a PC, not like passphrases for disk encryption; an examiner will not need to discover what the password is in order to bypass it.

Case Scenario: Activist Associations

Vera has lots of friends who are involved in controversial activism, and some of them have had their laptops seized at the U.S. border. Vera isn't an activist herself, but worries that the government will take an interest in her if it learns that she's friendly with people who are activists. She takes a travel laptop on an international trip with the minimum information necessary, leaving most of her data at home. Before she enters the United States, she signs out of her Gmail, Twitter and Facebook accounts and makes sure that the passwords aren't stored in her browser. She also uses WhisperCore's full disk encryption app to secure the contacts, text messages, and other content stored on her Android phone. If asked for the passwords, she intends to say no. She knows this might cause the agents to seize the devices, but they are unlikely to break the passwords, which are very strong. If that happens, Vera will still be able to access all the information on the devices because she has stored it remotely.

Temporary Phones for Travel

If your mobile phone uses the international GSM standard (usually the case for non-U.S. mobile subscribers, or for U.S. customers of T-Mobile and AT&T Wireless), you can avoid taking your normal phone on your international trip at all, even if you want to use your existing phone number.[43] Just get a different GSM-compatible phone and transfer your SIM card from your regular phone into the new phone. Your temporary phone will have far less of your private data on it, but since your phone number is associated with the SIM card rather than with the phone itself, you can still be reached at your normal telephone number (assuming that you have chosen to enable international roaming services on your cell phone account). When your trip is over, you can swap the SIM card back.

Secure Deletion of Data and Disk Encryption for Mobile Devices

It's very hard to be sure that information on mobile devices has been truly deleted. You might choose to delete information such as SMS messages so that they are not visible to someone looking through your phone, but there is typically no meaningful secure deletion option. A sophisticated forensic analysis may still reveal the contents of these deleted messages.

If your mobile device has a removable memory card such as an SD card, you can most securely wipe its contents by physically removing it from the mobile device and wiping it using secure deletion software in a PC.

In most cases, it may be better to travel with a separate mobile device that holds little private data rather than trying to rely on your phone's security features to prevent border agents from reading private data.

If you prefer to travel with your everyday mobile device, it may support specialized encryption software. The most recent release of Android for tablets (but not mobile phones) has a comprehensive encryption option, while some Android devices can be protected with add-on software like WhisperCore (which requires a fresh installation of the phone software)[44]. WhisperCore also supports making a networked backup of a phone's contents, securely erasing them, and re-downloading them later. BlackBerry devices also have potentially effective security options that may be able to protect data even against an expert; if you have an enterprise-managed BlackBerry, you can check out your user manual or ask your IT department about these features.

Digital Cameras

Agents may well ask to look through the contents of cameras, whether to try to disprove someone's claim about where they traveled, in search of sexually explicit photographs, or simply out of curiosity.

Be aware that border agents may search your camera, copy its contents, or try to undelete images or videos that you believe you've deleted and that are no longer visible from the camera's user interface.[45] There is no simple precaution against this, although low-level formatting or low-level overwriting a memory card in its entirety, using a computer and not a camera, should prevent undeletion; you should not rely on this unless you're familiar with exactly what the formatting process is doing. (Notably, high-level formatting of memory cards, or of hard drives, is totally ineffective against forensic analysis.)

The same considerations apply to camcorders and to the camera in your mobile phone.

Interacting with Border Agents

Border agents have a great deal of discretion to perform searches and make determinations of admissibility at the border. Keep in mind that any traveler, regardless of citizenship status or behavior, can be temporarily detained by border agents for more detailed questioning, a physical search of possessions, or a more extensive physical search.[46] Refusal to cooperate with searches, answer questions, or turn over passwords to let agents access or decrypt data may cause lengthy questioning, seizure of devices for further examination, or, in extreme circumstance, prevent admission to the country.[47]

For this reason, it may be best to protect your data in ways that don't require you to have awkward confrontations with border agents at all. If you find yourself in such a situation, however, keep these tips in mind:

Don't Lie

It's extremely important that you do not tell a lie to a border agent. Doing so is a serious crime for which you may be prosecuted even if your lie was not told to conceal any wrongdoing.[48] If you are absolutely sure that you don't want to answer a specific question, it's better to politely decline to answer than to give a false answer.

Don't Obstruct an Agent's Investigation

Once it's clear that a border agent is going to search your device or other possessions, don't take any steps to destroy data or otherwise obstruct that process. Like lying, knowingly interfering with a border agent's investigation is a serious crime.[49] Write down the agent's identifying information and collect a receipt for property if appropriate. Then file a complaint or consult a lawyer about getting the item back. (For information on filing a complaint to CBP or ICE, see the Appendix to this paper.)

Courtesy

It's in your interest to be courteous to agents at all times during the border inspection process. CBP agents should also be courteous and professional while searching your belongings, detaining, or questioning you.[50] If they fail to do so, you can file a complaint.

Appendix

Resources for International Travelers With Border Search Issues

Problems with or questions about an ICE or CBP examination?

If you have a question about CBP or wish to submit a formal complaint about a CBP examination, please go to <https://help.cbp.gov/app/forms/complaint>.

To file a civil rights complaint against either CBP or ICE, you can file a complaint with the Department of Homeland Security Office of Civil Rights and Civil Liberties. You may download a complaint form at <http://www.ice.gov/doclib/secure-communities/pdf/crcl-complaint-submission-form-english.pdf>.

Have you been repeatedly referred to secondary screening? Do you suspect your name is on a watch list?

You may submit a complaint to the Department of Homeland Security's Traveler Redress Inquiry Program at <https://trip.dhs.gov/>.

Want to know what information CBP or ICE has on file about you?

Anyone can seek copies of records about themselves through the Freedom of Information Act. You can use the Privacy Act to ask for the same information if you're a U.S. citizen or lawful permanent resident.

For information about submitting a request to CBP, see <http://www.cbp.gov/xp/cgov/admin/fl/foia/reference_guide.xml>.

To request records from ICE, see <http://www.ice.gov/foia>.

Feel as though your privacy or civil rights have been violated during a border search?

Please visit the Department of Homeland Security's Traveler Redress Inquiry Program to specify all scenarios that apply to your travel experience at <https://trip.dhs.gov/>.

Do you have further questions?

Contact an attorney for help.

Endnotes

[1] E.g., United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008); United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006); U.S. v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007); United States v. McAuley, 563 F. Supp. 2d 672, 979 (W.D. Tex. 2008); United States v. Roberts, 86 F. Supp. 2d 678, 688 (S.D. Tex. 2000); United States v. Bunty, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008); United States v. Hampe, No. 07-3-B-W, 2007 WL 1192365, at * 4 (D. Me. Apr. 18, 2007).

[2] See Electronic Device Privacy Act of 2008, H.R. 6588, 110th Cong. § 2(a) (2008); Travelers Privacy Protection Act of 2008, S. 3612, 110th Cong. § 4(a) (2008); Securing Our Borders and our Data Act of 2009, H.R. 239, 111th Cong. § 2(a) (2009).

[3] U.S. Customs and Border Protection, Dir. 3340-049, Border Searches of Electronic Devices Containing Information at 5.1.2 (Aug. 20, 2009), http://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.

[4] Id. at 5.3.1.

[5] Id. at 5.2.2. ("Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy.")

[6] Id. at 5.3.2.2.

[7] Id.

[8] U.S. Immigration and Customs Enforcement, Dir. 7-6.1, Border Searches of Electronic Devices ("ICE Directive") at 4, 6.1 (Aug. 18, 2009), <http://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf>.

[9] Id. 8.3.

[10] In one instance, ICE held onto David House's laptop, thumb drive, and digital camera for 49 days. An aquaintance of accused WikiLeaks whistleblower Bradley Manning, Mr. House was returning from Mexico when agents confiscated his electronic equipment. While the Justice Department conceded that it held onto his laptop for longer than thirty days, it explained that "[t]he lack of password access required ICE computer experts to spend additional time on Mr. House's laptop." Kevin Poulsen, Feds Defend Seizure of WikilLeaks Supporter's Laptop, Wired Threat Level (July 28, 2011) <http://www.wired.com/threatlevel/2011/07/house-lawsuit>.

[11] Id. at 8.4.

[12] ICE Directive, supra note [8], at 8.6.

[13] United States v. Cotterman, 637 F.3d 1068, 1070 (9th 2011) (petition for en banc rehearing filed Sept. 12, 2011) (permitting agents to transport a laptop to a forensic laboratory almost 170 miles away from the border and keep computer for two days to continue inspection, but the government "cannot simply seize property under its border search power and hold it for weeks, months, or years on a whim.").

[14] See, e.g., United States v. Hanson, No. CR 09-00946 JSW, 2010 U.S. Dist. LEXIS 61204 (N.D. Cal. June 2, 2010) (reasonable suspicion required to search laptop about two weeks after it was detained at the border and sent away for forensic analysis, and probable cause required to search laptop about four months after initial detention at border); United States v. Stewart, 715 F. Supp. 2d 750, 754-55 (E.D. Mich. 2010) (transporting a computer from an airport to a remote location might result in an extended border search). However, both of these cases rely significantly on United States v. Cotterman, No. 071207, 2009 U.S. Dist. LEXIS 14300 (D. Ariz. Feb. 24, 2009), which was reversed on appeal. 637 F.3d 1068.

[15] ACLU, Government Data About Searches of International Travelers' Laptops and Personal Electronic Devices (Aug. 25, 2011), http://www.aclu.org/national-security/government-data-about-searches-international-travelers-laptops-and-personal-electr.

[16] For example, Guidance Software markets a popular forensic analysis tool called EnCase, which "lets examiners acquire data from a wide variety of devices, unearth potential evidence with disk level forensic analysis, and craft comprehensive reports on their findings, all while maintaining the integrity of their evidence." EnCase Forensic, http://www.guidancesoftware.com/forensic.htm (last visited Oct. 4, 2011). Government

agents have used this tool to recover deleted files when searching devices seized at the border. See United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006) (finding the search to be reasonable under the border search exception). EnCase includes extensive functionality to help relatively non-expert users make sense of the contents of a hard drive, including, for example, finding and reading the content of email messages. Computer forensic tools will become more automated in the future; see Simson Garfinkel, "Automated Computer Forensics" (available at <http://simson.net/page/Automated_Computer_Forensics>).

17 "SpiderOak is a 'zero knowledge' backup provider. This means that we do not know anything about the data that you store on SpiderOak -- not even your folder or filenames. On the server we only see sequentially numbered containers of encrypted data." <https://spideroak.com/faq/questions/3/does_spideroak_use_encryption_when_storing_and_transferring_data/>.

18 "Backups should be secure against attackers ranging from "script kiddies" up to major world governments, even if they can compromise the systems on which the backups are being stored. Backups are supposed to be a tool for mitigating damage — not a potential vulnerability to worry about!" <http://www.tarsnap.com/design.html>.

19 "[I]n stark contrast to most other online storage services, all your files get encrypted on your computer, so that no one - including the employees at Wuala and LaCie - can access your private files. Your password never leaves your computer." <https://www.wuala.com/en/learn/technology>.

20 Duplicity is available from <http://duplicity.nongnu.org/>.

21 Tahoe-LAFS is available from <https://www.tahoe-lafs.org/>.

22 See United States v. Seljan, 547 F.3d 993, 999 (9th Cir. 2008) (en banc).

23 Nicole Perlroth, "Traveling Light in a Time of Digital Thievery," New York Times, February 11, 2012, <https://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html>.)

24 For convenience, computer users prefer to have important data immediately available on their mobile devices (without having to download it); likewise, they prefer to be able to access on-line resources quickly and easily (without having to constantly re-authenticate themselves in cumbersome ways). Both of these desires are in tension with the goal of protecting sensitive information when mobile devices could be lost, stolen, seized, or secretly tampered with. Travelers would be be safer with devices that store much less sensitive information locally, and that possess less permanent authority to access sensitive online resources.)

25 Alexei Czeskis, David J. St. Hilaire, Karl Koscher, Steven D. Gribble, Tadayoshi Kohno, and Bruce Schneier, Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications, available at <https://db.usenix.org/event/hotsec08/tech/full_papers/czeskis/czeskis.pdf>.

26 See <http://simson.net/ref/2006/>.

27 Undeletion is a standard, built-in feature of forensic products used by law enforcement and border agencies. It works reliably if deletion was done recently. It may work even after an operating system reinstallation ("slack space"), depending on how the reinstallation process works. (However, it typically doesn't work after OS reinstallation if full-disk encryption was used on the previous OS image, because the new operating system will overwrite the decryption keys and make the old system's encrypted data unrecoverable.)

28 DBAN is available from http://www.dban.org/.

29 Czeskis et al. point out that the operating system and applications can leak significant information about the existence of, and the files stored within, a hidden volume:

> [These risks] also seem applicable to regular (non-deniable) disk encryption systems in which only a subset of all the user's entire disks are encrypted and in which a user does not deny the existence of the encrypted regions but does refuse to divulge the passwords. [...] In summary with regard to disk encryption, in situations where there is a need to protect the privacy of individual files, the safest strategy appears to be to encrypt the full disk [...]

For example, the authors found that Microsoft Word would periodically auto-save copies of a document being edited. Even if the document being edited was located on an encrypted volume, Word could place the auto-saved copies on an unencrypted volume; even though they were automatically deleted, these copies could easily by undeleted by a forensic examiner. (In a similar vein, applications may create and store a "preview" or "icon" version of documents and images they open.) Supra note [23].

30 https://twitter.com/#!/csoghoian/status/75793191177166849 ("4GB SD cards are cheap, can be destroyed before going through US customs, and by taking out my [hard drive], my laptop battery now lasts 8 hrs.")

31 See <https://secure.wikimedia.org/wikipedia/en/wiki/Comparison_of_disk_encryption_software>.

32 See EFF's DES Cracker page: <https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html>.

33 For a useful general discussion of passphrases, see Indiana University UITS, "Passwords and Passphrases", available at <http://kb.iu.edu/data/acpu.html>, and "Passphrases", availalbe at <http://protect.iu.edu/cybersecurity/safeonline/passphrases>. These documents are not specifically focused on passphrases for disk encryption; bear in mind our warning, infra note [34].

34 Arnoud Engelfriet, The Passphrase FAQ, available at <http://www.iusmentis.com/security/passphrase-faq/>.

35 See Reinhold's Diceware page at <http://world.std.com/~reinhold/diceware.html>.

36 xkcd #936, available at <https://www.xkcd.com/936/>. Note that this phrase is likely too short for disk encryption use; Munroe calculates its strength at only 44 bits. Reinhold's advice suggests using at least five random words for a passphrase for encryption purposes, when the words are chosen from a list that includes only simple everyday words. Exactly how long or unpredictable a passphrase needs to be to be secure against cracking by machines is a complex question, and relies on speculation and assumptions about the capabilities of the organizations that will try to crack your passphrase. Some disk encryption systems can be safe even with relatively short passphrases because of how they use key stretching technologies; see <https://en.wikipedia.org/wiki/PBKDF2#Disk_encryption_software>. But you should not use this as an excuse to choose a simpler passphrase unless you understand the precise technical details of how the disk encryption software you've chosen uses key stretching. Note that this comic is licensed under a Creative Commons Attribution-NonCommercial 2.5 License.

37 Simply using a quotation or song lyric by itself is not safe because there are readily available lists of quotations and lyrics, comprising only millions of distinct sentences. This is a tiny number for a computer to test. Your passphrase should never be identical to anything that has ever been published anywhere.

38 <http://point-at-infinity.org/ssss/>.

39 <http://sourceforge.net/projects/secretsharp/>.

40 See In re Grand Jury Subpoena to Sebastien Boucher, 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007), appeal sustained by 2009 WL 424718 (D. Vt. Feb. 29, 2009); United States v. Rogozin, 09-CR-379, 2010 WL 4628520 at **5-6 (W.D.N.Y. Nov. 16, 2010); United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355 (E.D. Mich. March 30, 2010); United States v. Fricosu, ____ F. Supp. 2d ____, 2012 WL 182121 (D. Colo. Jan. 23, 2012); In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, ____ F.3d ____, 2012 WL 579433 (11th Cir. Feb. 23, 2012).

41 This should become far easier and more routine in the future, as suggested by Roxana Geambasu, John P. John, Steven D. Gribble, Tadayoshi Kohno, and Henry M. Levy Keypad: An Auditing File System for Theft-Prone Devices, in Proceedings of the European Conference on Computer Systems (EuroSys), Salzburg, Austria, April 2011, available at <http://eurosys2011.cs.uni-salzburg.at/pdf/eurosys2011-geambasu.pdf>.

Geambasu et al. describe an encryption system where a network server, rather than an end-user, holds the keys. Under normal circumstances, the server will immediately provide the keys to decrypt any file that a user wants to use, but the server operator can temporarily or permanently revoke a device's ability to request decryption keys (for example, if the device is lost). When practical implementations of this system become available, they could be ideal for border crossings, because a server can turn off decryption key access for a traveler's laptop at a given time and re-enable it only after the traveler has passed through immigration and customs.

42 Michael Wei, Laura M. Grupp, Frederick E. Spada, and Steven Swanson, Reliably Erasing Data From Flash-Based Solid State Drives (in Proceedings of the 9th USENIX Conference on File and Storage Technologies), available at <https://db.usenix.org/events/fast11/tech/full_papers/Wei.pdf>. Wei et al. note that, "[t]he internals of an SSD [solid state drive] differ in almost every respect from a hard drive, so assuming that the erasure techniques that work for hard drives will also work for SSDs is dangerous."

43 Not all mobile service plans support using your SIM card in a foreign country. If in doubt, contact your mobile phone carrier.

44 As of February 2012, WhisperCore was unavailable following the acquisition of Whisper Systems by Twitter.

45 "Deleted" photos on cameras are generally not really erased, and can be trivially undeleted using a computer and widely available software. Undeleting photos from a camera's memory card does not usually require special technical expertise or forensic training.

46 See Inspection of Electronic Devices, supra, note [19] at 1; U.S. Customs and Border Protection, Reasons You May Be Searched By CBP, https://help.cbp.gov/app/answers/detail/a_id/26/kw/border%20search (last visited Oct. 4, 2011).

47 For example, the government may refuse non-citizens entry into the U.S. for a variety of reasons. Immigration and Nationality Act § 212(a), 8 U.S.C. § 1182 (2010). While few judges have shed light on the issue, at least one court has found that U.S. citizens have an "absolute and unqualified right" to reside in the United States and cannot be denied reentry. United States v. Valentine, 288 F. Supp. 957, 980 (D.P.R. 1968); see also Worthy v. United States, 328 F.2d 386 (5th Cir. 1964) ("We think it is inherent in the concept of citizenship that the citizen, when absent from the country to which he owes allegiance, has a right to return, again to set foot on its soil.").

48 18 U.S.C. § 1001 (2006) (it is a crime to willfully or knowingly "falsif[y], conceal[], or cover[] up by any trick, scheme, or device a material fact" or make "any materially false, fictitious, or fraudulent statement or representation" to a federal agent).

49 18 U.S.C. § 1519 (2006) (it is a crime to "knowingly alter[], destroy[], mutilates[], conceal[], cover[] up, falsif[y], or make[] a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States[.]"

50 U.S. Dep't of Homeland Security Customs and Border Protection, Inspection of Electronic Devices at 1, http://www.cbp.gov/linkhandler/cgov/travel/admissibility/msa_tearsheet.ctt/msa_tearsheet.pdf (last visited Oct. 4, 2011) ("If you are subject to inspection, you should expect to be treated in a courteous, dignified, and professional manner.").