Laptop and Electronics Searches at the U.S. Border

Seth Schoen and Marcia Hofmann

Electronic Frontier Foundation

white paper

- First published in December 2011
- Joint work of Seth Schoen (EFF senior staff technologist) and Marcia Hofmann (EFF senior staff attorney) combining legal and technical perspectives re: searches of devices at the U.S. border
- Quite a bit of bad news

The border is a difficult place

- High-stress, sometimes confrontational situation
- Exceptions to familiar rules about rights when dealing with law enforcement
  - Search and seizure rules
  - The right to have an attorney present during questioning

the law

"reasonable" search (1)

- The Fourth Amendment to the United States Constitution: "the people [shall] be secure . . . against unreasonable searches and seizures" by the government
- But courts have held that searches occurring at at the border are automatically reasonable

"reasonable" search (2)

"The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, we have stated that searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."

United States v. Flores-Montano, 541 US 149 (2004)

legal challenges

- Organizations including EFF have argued in court for limitations on border searches of electronic devices
- So far, courts have been unsympathetic to these arguments and reluctant to limit these searches.
  - *See, e.g., U.S. v. Arnold*, 533 F.3d 1003 (9th Cir. 2008)
- Current cases: *House v. Napolitano, Abidor v. Napolitano*

agencies

alphabet soup

- TSA: handles domestic security; searches you before you get on a plane in the U.S.
- CBP: primarily responsible for border inspection
- ICE: enforcement agency; primarily investigates immigration and customs violations, but has authority at the border
- INS: doesn't exist anymore

some powers of border agents

WITHOUT reasonable suspicion, can:

- Detain you temporarily (up to a few hours)
- Seize possessions temporarily, including devices to analyze or copy them
- Ask lots of questions (though only a judge can actually compel an answer)
- Refuse admission

border search policies: CBP

Customs and Border Protection agents can inspect electronic devices and data at the border "with or without individualized suspicion."

- May keep for a "brief, reasonable" time
- May send device or data to other another agency to seek help, e.g., with technical issues or decryption
- Unclear how privileged or sensitive data is handled

border search policies: ICE

Immigration and Customs Enforcement agents follow a similar policy.

- Can also inspect "with or without individualized suspicion"
- Will generally complete searches within 30 days, but anecdotes suggest it can take much longer
- May also seek technical help from other agencies
- Also unclear how privileged or sensitive data is handled

strategies

first, assess and prepare

personal considerations (1)

- Your citizenship, immigration, or residence status
- Time sensitivities
- Your tolerance for hassle from border agents
- How important it is for you to have access to data during your journey

personal considerations (2)

- How good your internet access will be during your travels
- The places you've visited on your trip before entering the country
- Your history with law enforcement

choosing not to answer questions

- Can have adverse consequences: temporary detention, heightened scrutiny on future border crossings, refusal of admission
- Preferable to have (genuine) external reasons for not answering, such as an employer's policy or one's professional responsibility to others

basic precautions before travel

Keep regular encrypted backups elsewhere

Encrypt the storage media you're taking on your trip

Or use only network storage

strategy 1:
don’t bring what you don’t need

don't carry data with you (1)

- Separate travel OS image(s)
  - Make image backup of your disk (e.g. with dd; beware of bad sectors) before your trip, then [wipe and] install a new, separate OS for travel
  - Use a separate hard drive for travel
  - Remove hard drive and use external media to boot (live CD, USB, SD card)

don’t carry data with you (2)

- Upload data from one place and download it later
- You can try to automate this using a device like a Chromebook that automatically (primarily) stores things on a network server
- Consider issue of service provider access (prefer to separately encrypt everything before uploading)

don’t carry data with you (3)

- Send laptops or (encrypted) media separately by mail/common carrier
  - Still subject to search by Customs inspectors (potentially even including letters not bearing a Customs declaration form)
  - But at least those inspectors aren't detaining and interrogating you while they perform the search!
  - Probably no authority to alter/bug equipment without a warrant

strategy 2: encryption

password strength (1)

Oov6pie.
Vie;h*a7
sai'Sh1i
ooy9AiB&

- These passwords are horribly inadequate as cryptographic keys. E.g., EFF's DES Cracker could brute force them in 1998.

password strength (2)

- Today, rainbow tables already strain limits of humans' memory and patience for random password strings
- Government probably has better cracking capability than you :-)
- Traditional suggestion: passphrases based on slightly altered individually-meaningful texts, e.g. lyrics, quotations, slogans

password strength (3)

- Online vs. offline attack: brute force rates separated by many orders of magnitude
- xkcd observation: you can remember several words (with high net entropy) better than !X87m6e_,o97kdD0/LPK#Xs-
  - To defend only against online attack, their recommendation (Reinhold's Diceware-style) gets to only 2^{44} possibilities which is still not enough against offline attack
  - Use more words! :-)

password strength (4)

```
#!/usr/bin/env python
 import random, math
 d = open('/usr/share/dict/words').readlines()
 n = 5
 print ' '.join(random.choice(d).rstrip() for i in range(n))
 print n * math.log(len(d))/math.log(2), 'bits'
```

- If you don't like some of the words,
  d = [w for w in d if good(w)]
- If your disk crypto uses PBKDF2 well, you need fewer bits
- I wonder how random random.choice() is

forced decryption (1)

- In the United States, only a judge can force a person to reveal information to the government, and only where the person doesn't have a valid constitutional right against self-incrimination.
- But remember: this isn't the case in all countries!

forced decryption (2)

- Know that refusing to provide information can have adverse consequences, *e.g.*, refusal of admission
- Consider before your trip how you will deal with requests to decrypt
- IT policies can be helpful—don't let travelers know their passwords until they reach their destinations

not knowing the password (1)

- Manually change disk passphrase to something random you can't remember and send via separate channel
  - You have lots of choices about what that channel should be, with different security and convenience tradeoffs
  - Encrypted e-mail? To yourself or someone else? Store it on a server? Have someone else carry it? Send it in a letter? …

not knowing the password (2)

- Great design by Roxana Geambasu *et al.*, "Keypad: An Auditing File System for Theft-Prone Devices" (EuroSys 2011)
  - Files individually encrypted, server knows keys and can log access to individual files
  - Access to files can be turned on and off at will by server operator
  - Precautionary "self-DRM"?

not knowing the password (3)

- Need a production implementation of Keypad
  - Auditing feature (what, exactly, did someone look at)?
  - Control feature (deny accesses to files when device is out of owner's control)
- Similar technique is also possible at the whole-disk level; and Google could and should also do it for ChromeOS

not knowing the password (4)

- We can do this in a more general and automated fashion
- Making physical possession of a device (and knowledge of password) not solely determinative of access, with low network overhead
- Parallels to existing MAC, DRM (!), and multifactor authentication concepts

special considerations

tl;dr:

deletion is hard

forensics is effective

secure deletion

- High-level delete and format commands often don't clear low-level data
  - cf. Simson Garfinkel's used hard drives
- Even “secure delete” and “clear empty space” may not; modern log structured filesystems may prevent overwriting blocks in-place, or preserve old revisions as if still allocated
- So can wear leveling on flash drives

wiping an entire drive

- Peter Gutmann's suggestions about multiple-pass overwrites are now considered obsolete, including by Gutmann
  - At least for magnetic-platter hard drives
- For most threat models, single-pass dd should wipe magnetic drives safely. And you might actually do it! :-)
- Different from securely deleting a file because filesystem structure is irrelevant.

encrypted volume leakage

- If you encrypt something other than your full local hard disk, applications or parts of your OS might leak filenames (or much more) from the encrypted side to the unencrypted side
- Alexei Czeskis *et al.*, "Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications" (HotSec 2008)

device-specific considerations

mobile devices

- Mobile devices: *best* area for forensics, *worst* for counterforensics
- Most have no full-disk encryption, no secure erase; it's commonly hard to add these yourself
  - Some exceptions (Blackberry with Enterprise Server; Whispercore; most recent Android)
- Powerful, readily available forensic tools

cameras

- Border agents might search or copy contents of cameras too
- Cameras don't provide a secure delete function, and deleted photos can even be undeleted with a simple FAT undelete program
- Using your computer to erase SD cards (perhaps with multiple overwrites)

interacting with border agents

tips

- Avoid giving border agents excuses to get curious/alarmed about you and your possessions
- Do not lie to border agents
- Do not obstruct an agent's investigation
- Do be polite to them

beyond the U.S. border

- Other jurisdictions may take an even more expansive view of border search authority
  - *e.g.*, prohibiting importation of encrypted data or considering it suggestive of espionage
- Travelers often suffer theft of their digital devices
- Some travelers are themselves targets of corporate or state espionage

ELECTRONIC FRONTIER FOUNDATION eff.org

questions or comments?

Contact:

Seth Schoen <schoen@eff.org>

Marcia Hofmann <marcia@eff.org>

PGP keys on EFF web site

https://www.eff.org/