The Surveillance State and what to do about it

Steve Revilak
https://masspirates.org/

Boston Anarchist Bookfair

Nov 21, 2015

First Principles

surveillance (n) Close observation of a person or group, esp. one under suspicion.

- Surveillance is a form of oppression
- Surveillance is a form of social control
- Surveillance does not make you safe

Second Principles

- At the federal level, US intelligence agencies are heavily invested in surveillance. Think NSA and Edward Snowden, or the FBI and COINTELPRO.
- At a state level, law enforcement agencies engage in surveillance. Think BRIC.
- Large Corporations are heavily invested in surveillance. IMHO, there is not a meaningful difference between corporate and state surveillance.
  - Corporations can be asked (or compelled) to turn over information they have. Some (e.g., AT&T) are willing and eager to do so.
  - Intelligence agencies piggyback on corporate surveillance. (e.g., the NSA's use of tracking cookies).

Counter-Surveillance 101

- Counter-surveillance = things you do to prevent surveillance (or, to make surveillance more difficult)
- It really boils down to information security and risk management.
  - What "risks" do you care about
  - How much effort are you willing to spend

Paper

Shredding

- Old-school recycle bin diving is still an effective method for gathering information.
- But, hard to do at scale
- In fact, it's really hard to do mass surveillance on paper.

Tip: shred paper before putting it out on the curb.

Story: Adobe, e-readers and DRM

Credit Cards, Discount Cards

Credit cards

- A record of each financial transaction you make
  - Where you shopped
  - How much you spent
  - If you pay in person, also a record of where you were, and when.
- Some tech, phone companies publish transparency reports
  - Have you ever seen a transparency report from a bank?

The same applies to any card tied to "you". The card generates records about what you do, and paint a picture of who you are.

Tip: cash is a good thing.

Cookies

- Cookies are little bits of "state", and they make the web work. They're also a vehicle for surveillance.
- First Party Cookies: these are sent to the web site you're visiting. They're generally necessary.
- Third-Party Cookies: these are sent to some other website. They generally involve marketing, ad-brokering, analytics, and other forms of corporate surveillance. Avoid them.

Demonstration: facebook.com, huffingtonpost.com, and the `datr` cookie. This is how companies track you on the web.

Fun: Tamper Data

Email

Think about the email message your friend sends, and what a marketer sends. How are they different?

- Tracking pixels

  ```
  <img src="http://www.gradienter.xyz/a62JX85Ae8fkmOnn.."
  ```

- This came from a piece of spam, but the alphabet soup is still a tracking token.
- UTM: Urchin Tracker Module, aka Google Analytics

  ```
  <http://www.mailchimp.com/monkey-rewards/?
     utm_source=freemium_newsletter
     &utm_medium=email&utm_campaign=monkey_rewards>
  ```

Fun: How to forge an email address

Social Media

There are three things to remember about social media:

1. It's public
2. It's public
3. The cops read it

Social networking sites are in the advertising business, period.

They're useful for advertising and mobilizing. They're a poor choice for organizing and planning.

Story: my day at the airport

Story: lyrics + facebook = prison time

Smart Phones

Currently not a happy story.

- Your phone is a little computer. It's got a microphone that can be turned on remotely.
- When powered on, it pings cell towers. This generates a record of where you were, and when.
- Apps that ask for access to contacts, SMS, GPS – and then phone home with the information.
- IMSI catchers (aka Stingrays)

For many people, a smart phone is their only source of internet access.

Discussion: do you see the irony there?

Encryption

Encryption is the process of encoding a message, so that only the intended recipient can read it.

To anyone else, the message looks like gibberish.

Fine Point: technically, encryption is the process of encoding a message so that only the party with the correct *key* can read it. (Leap of faith involved).

Encryption Keys

Encryption keys come in pairs.

- There's a **public key**. You can give this to everyone
- There's a **private key**. You give this to no-one.
- Anyone can use a public key to encrypt a message.
- Only the person with the private key can decrypt it.

decrypt(privateKey, encrypt(publicKey, MSG)) = MSG

HTTPS: a popular encryption scheme

Think of the little lock icon in your web browser.

- The web server has a private key.
- The web server sends you the public key.
- You use the public key to encrypt traffic to the web server.
- Result: The web server can decrypt your traffic. Someone collecting traffic off the network can't decipher it.

Discussion: This shows how your *request* to an https site is encrypted. The web site sends back a web page. How is that *response* encrypted?

Digital Signatures

Earlier, we saw how easy it was to forge an email address.

By contrast, forging digital signatures is extremely hard.

Basic Recipe:

- You have a private key
- You use your private key to create a digital signature.
- Anyone with your public key can verify the signature.

Story: Patent trolls, lawyers, and discovery

Discussion: Browser HTTPS warnings (aka "who do you trust"?)

Pretty Good Privacy aka PGP

Pretty Good Privacy:

- A system for encrypting email messages (and other kinds of data).
- Supports encryption (only the recipient(s) can read it)
- Supports digital signatures (you can verify the sender is who they claim to be)
- Popular implementations: GnuPG with Thunderbird and Enigmail

Story: Crypto wars vs Free Speech

OTR – off the record messaging

- Commonly used with chat protocols.
- Both parties generate a one-time key.
- You use the key to communicate
- At the end of your session, the key is thrown away.

This provides a useful property called *Perfect Forward Secrecy*. If someone were to break (or guess) an OTR key, they'd only be able to decrypt one conversation, not all conversations.

Disk encryption (or device encryption)

- FileVault on Mac OS, LUKS on Linux, BitLocker on Windows.
- The entire contents of your disk is encrypted.
- You'll need to provide a password (a decryption key) in order to access your files.
- Absolutely a good thing to use.

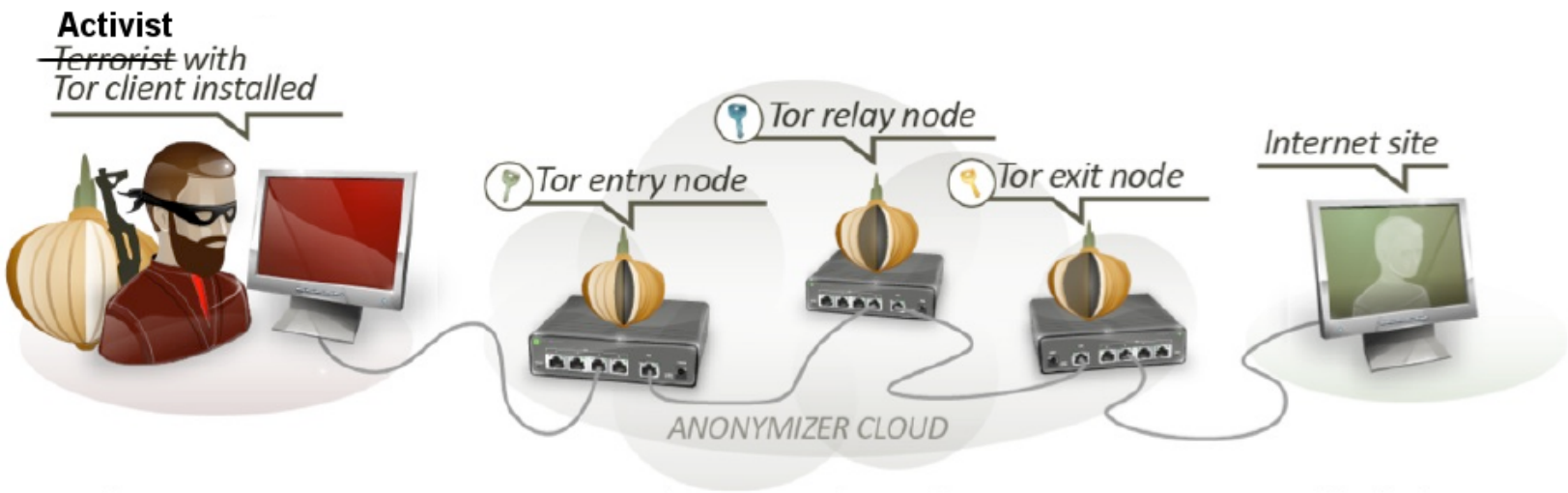
If someone steals your laptop (or device), they get the hardware; they don't get the data.

Tor: The Onion Router

- A program (and a network) for preserving privacy on the web.
- Aside from encryption, Tor also provides anonymity.
  - The web site you visit can't determine your IP address.

Discussion: Packets and envelopes.

How Tor Works



Fun: Tor, GeoIP, and MaxMind

VPNs (Virtual Private Networks)

- Normally, traffic goes from your computer $\Leftrightarrow$ service provider.
- With VPN, traffic goes from your computer $\Leftrightarrow$ VPN Gateway $\Leftrightarrow$ service provider
  - Service providers see your VPN gateway address, and not your real IP address.
  - Traffic between your computer and the VPN gateway is encrypted.
- Very useful when traveling, or when using open WiFi networks.
- Anonymity guarantees aren't as strong as Tor.

Tip: in a pinch, ssh is a useful VPN

Password Managers

- The more important the information, the stronger (aka longer) your password should be.
- It really is better to use different passwords for different websites/services.
- Don't try to remember them all. Use a password manager.
- Password managers store your passwords in an encrypted file.
- Password managers can generate random passwords for you

KeepassX is a pretty good one.

Story: The one byte XOR password

Free Software

Socially responsible software.

0. You're free to install and run the software, on as many computers a you wish, for any purpose that you wish
1. You're free to examine the source code, to see how the program works.
2. You're free to change the source code (and thereby change how the program works)
3. You're free to redistribute your modifications.

Free software licenses list all the things you're allowed to do.

Proprietary software licenses list all of the things you're not allowed to do

Is Free Software Better, More Secure, etc

- Lots of free software is very high quality; some of it isn't.
- Not a guarantee of better security (but perhaps likely to provide more privacy)
- Free vs. non-free is more a social choice than a technical one.

It's hard to backdoor a program when the source code is public.

Useful Resources: The web

Web browser plugins (for Firefox and/or Chrome):

- NoScript.
  `https://noscript.net/`
- HTTPS Everywhere.
  `https://www.eff.org/HTTPS-everywhere`
- RefControl
  `https://addons.mozilla.org/en-us/firefox/addon/refcontrol/`
- Tamper Data
  `https://addons.mozilla.org/en-US/firefox/addon/tamper-data/`

Useful Resources: The web (cont'd)

- Privacy Badger
  `https://www.eff.org/privacybadger`
- Terms of Service; Didn't read
  `https://tosdr.org/`
- Lightbeam
  `https://addons.mozilla.org/en-US/firefox/addon/lightbeam/`
- The Tor Project
  `https://www.torproject.org/`

Useful Resource: Email

- GnuPG
  `https://gnupg.org/` (Main site)
  `http://www.gpg4win.org/` (Windows)
  `https://gpgtools.org/` (Mac OS)
- Enigmail
  `https://www.enigmail.net/home/index.php`
- Thunderbird
  `https://www.mozilla.org/en-US/thunderbird/`

Useful Resources: General

- Surveillance Self Defense
  `https://ssd.eff.org/`
- PRISM Break
  `https://prism-break.org/en/`
- The Guardian Project
  `https://guardianproject.info/`
- Cryptoparty
  `https://www.cryptoparty.in/`

Random

- Acxiom's "About the Data"
  `https://www.aboutthedata.com/`

Conclusions

- There's a lot of stuff in here. Don't be overwhelmed. Pick something; tinker with it.
- Resistance is not futile!
- How to beat surveillance? Make it incrementally harder for people to do it.
- There aren't absolutes. Experiment, find what works for you.

Counter-surveillance (aka *privacy*) is like locking your front door. There's nothing wrong with locking your front door.