Protecting Your Privacy in the Digital Age

Steve Revilak

Software Freedom Day

Sep. 21, 2013

State Surveillance

- Over the summer, we've learned about a number of NSA programs that spy on . . ., well, just about everyone.
- Examples: NSLs, PRISM, XKeyScore, BULLRUN, Tracfin/FTM.
- Closer to home, we have automatic license plate readers (ALPRs), and an explosion in surveillance camera deployments.
- Invasive. High creepy factor.

Corporate Surveillance

- We have tech companies: Google, Facebook, Microsoft
  - “Pressure cooker” + “backpack” = SWAT Team
  - Will they hand over your data in response to a subpoena? Will they notify you?
- Mobile devices
  - Location tracking
  - “Four-hundred-thousand apps means 400,000 possibilities for attacks.” (quote attributed to Michael Hayden)
- Internet Service Providers
  - Record all of your HTTP requests? Pen Registers for the digital age?
- Analytic Marketing (aka “web stalking”)
- Aggregators: Intellius, Acxiom

State + Corporate Surveillance

Quote from one of the documents leaked by Edward Snowden:

> *As far back as World War II, NSA has had classified relationships with carefully vetted U.S. companies that assist with essential foreign intelligence-gathering activities. NSA maintains relationships with over 100 U.S. companies. Without their cooperation, NSA would not be able to respond to intelligence requirements on a variety of topics important to the United States.*
>
> *(March 2009 OIG report)*

Takeaway: Collaboration with private companies is critical to the government surveillance efforts. In some cases, corporate surveillance has equated to government surveillance.

The Age of Big Data

- Data collection is one aspect of surveillance.
- We're in the age of "big data". There are facilities for storing, querying, and analyzing all of this stuff.
- Big surveillance is what justifies the cost of storing and managing big data.

What to do, what to do . . .

- From a privacy standpoint, this whole thing kind of stinks.
- You'd like to protect your privacy; where do you start?
  - In all seriousness, start anywhere.
  - Assume that no strategy is perfect.
  - Protecting privacy ≈ counter-surveillance.
- Two ways of approaching the dilemma.
  - Figure out what risks are most important to you. Work on them first.
  - Figure out what risks are easiest to address. Work on those first.

Remember: All resistance is positive.

Privacy, Security, and Risk Management

- Protecting your privacy is a form of data security.
- Security is a form of risk management.
- Risk management is about making trade-offs.
  - What's the cost of bad things that might happen?
  - What's the probability that bad things will happen?
  - What's the cost of the countermeasures?
  - How effective will the countermeasures be?
- There's no simple recipe for security (or privacy). You'll have to think through your own situation, and you'll have to make trade-offs.

Avoid Dumpster Divers

- Don't overlook the simple, low-tech stuff
- If you put it out in the trash, it's up for grabs.
- Get a shredder. At a minimum, shred anything with your name on it.
- Ditto for old hard drives. Securely wipe or physically destroy the media. Or both.
- Don't leave snail mail exposed to the public.

Loyalty/Rewards Cards

- These are the cards that CVS, Stop & Shop, ACE, etc. ask you to scan at the checkout register.
- They are not "rewards": they are surveillance in exchange for discounts. (i.e., anti-features)
  - Question: which stores penalize shoppers who decline to participate in their surveillance programs?
- What could a company do with a complete purchase history from their store? What could they combine that data with? Who could they sell it to? Could knowing your shopping habits make you more susceptible to social engineering?
- Aside from purchase history, these cards reveal where you were, and when.

ATM and Credit Cards

- In 2011, the NSA collected some 180 million VISA transactions. (Der Speigel)
- Aside from revealing your purchase history, using plastic reveals where and when you shopped.
- Use cash.
  - Yes, you can be mugged when carrying cash, but
  - you can also be mugged and forced to make withdrawals using your ATM card.
- Don't stiff your favorite merchant by forcing them to pay transaction fees.

Cell Phones

- Bad reception and dropped calls are the least of your worries.
- Cell phones are little computers, that are always connected to a network. Try thinking in these terms:
  - Software (aka apps) $\Leftrightarrow$ Vulnerabilities
  - Connected $\Leftrightarrow$ Exposed
- Aside from data on your cell phone (texts, contacts, calendar, call history, etc), cell tower triangulation can provide an accurate record of your location.
- Plus, they have microphones which can be turned on remotely. ("Look mom, I'm wearing a wire")
- Suggestion: as much as possible, turn the phone off. Pull out the battery out or keep it in a Faraday bag.
- Be suspicious of apps that you install.

Feeding the Cookie Monster (1)

- Cookie: a Netscape hack that added state to the HTTP protocol.
  - Cookies make the web work.
  - Cookies also make web surveillance very easy.

Let’s examine the surveillance aspect in some detail.

Feeding the Cookie Monster (2)

- Let's say I view Facebook.com's homepage. My browser sends this:

  ```
  GET / HTTP/1.1
  Host: www.facebook.com
  ```

- Facebook responds with

  ```
  HTTP/1.1 200 OK
  Set-Cookie: datr=J_dcT9Ig73PaZ1Wus3EHA3IJ; \
    expires=Tue, 11-Mar-2014 19:04:07 GMT; \
    path=/; domain=.facebook.com; httponly
  ```

Feeding the Cookie Monster (3)

- `datr=J_dcT9Ig73PaZ1Wus3EHA3IJ` looks harmless. But happens when I go to huffingtonpost.com?

  ```
  GET /dialog/oauth?... HTTP/1.1
  Host: www.facebook.com
  ...
  Connection: keep-alive
  Referer: http://www.huffingtonpost.com/
  Cookie: datr=J_dcT9Ig73PaZ1Wus3EHA3IJ;
  ...
  ```

- Facebook just “followed” me to huffingtonpost.com via embedded code (note the “Referer” and “Cookie” headers).

Feeding the Cookie Monster (4)

Suggestions:

- Do not accept third-party cookies.
- Have your browser clear history, cookies, and form data when it closes.
- To the greatest extent possible, configure your browser not to send referer headers.
- Advanced: use NoScript (or similar) to block JavaScript (again, to the greatest extent possible).
- If you need to stay logged in to a web service for long periods of time, do it in a dedicated browser (or private browsing window). Don't use the dedicated browser (or private browsing window) for general web surfing.

Watching the Watchers

This is a fun exercise!

- Turn off the privacy-enhancing extensions in your web browser (HTTPS Anywhere, NoScript, Ad Blockers, etc).
- Run one of these commands

```
sudo tcpdump -s 1500 -l -A dst port 80
sudo tshark -O http -i eth0 -s 1500 \
   -f "dst port http" -d "tcp.port==80,http"
```

- Browse the web, and watch the output. (Look for the words “GET”, “POST”, and “Host”.)

Email & ECPA

- Electronic Communications Privacy Act (ECPA)
- Mail stored on a third-party server for more than 180 days is considered abandoned. Such messages can be obtained without a warrant, and without judicial oversight.
- Might have made sense in 1986, when the law was written. Creates significant individual exposure today.
- Suggestion: download old messages and store them locally; don't keep them on third-party servers.

Email and Your Email Service Provider

- How will your ESP respond to a government request for information?
  - Will they defend you?
  - Will they bother to tell you about it?
- Who provides your email service?
  - An organization that's in the business of providing email hosting, and (perhaps) charges for their service, or
  - a company that gives you free email hosting, in return for the privilege of surveiling you?
- In 2012, one major ESP made 96% of their revenue by selling advertising. They're (arguably) in the business of surveillance.
- Suggestion: look at your ESP's policies, especially surrounding secondary use (aka "sharing"). If you don't like the policies, move your data.

Email and Encryption

- Properly implemented strong encryption is an effective way to thwart surveillance.
- Learn how to use GnuPG (a free implementation of the OpenPGP standard).
  - The initial setup can be a bit tricky.
  - Once you get past the initial setup, PGP is very easy to use.
- ~~I've got nothing to hide~~. You've got nothing to see.
- Sign messages for non-repudiation, and to verify your identity.
  - You too can be compelled to hand over 20,000 email messages to a lawyer.

Other technologies

- Use Tor to anonymize your web browsing.
  - Tor hides the source of traffic.
  - Tor changes routes roughly every 10 minutes.
- Use Virtual Private Networks
  - Encrypts traffic.
  - Hides you among other users of the VPN service.
- Use OTR (off the record) encryption for chats.
  - Short-term encryption keys.
  - Perfect forward secrecy. Knowing one key tells you nothing about previous (or subsequent) keys.
- Use HTTPS as much as possible.
  - Government agencies may be in cahoots with members of the certificate cartel.
  - (Arguably) better than no encryption at all.

Low-tech Approaches

- Send a letter instead of sending an email.
  - Snail mail is slower, but it's more tamper-evident than email.
- Talk things out face to face
  - but be careful with those cell phones.

Once again, all resistance is positive.

Surveillance Cameras

- Over the last few years, surveillance cameras have become pervasive.
- What can you do about them?
  - Wave?
  - Shine a green laser pointer at them?
  - Hide in the bathroom? (for now)
  - Be glad you're not in the UK? (for now)
- Sorry, no good tips for visual counter-surveillance.
- We can advocate for written policies regarding data access, data retention, and third-party use.
- Wireless cameras can be fun, if you have the right wireless receiver.

Hacking Privacy Policies

- This is a creative exercise, and a fun way to kill an afternoon.
- Get a copy of some website's privacy policy, preferably from a website run by a large publicly-traded company.
- Read the privacy policy.
- Put on your "I'm a greedy capitalist who wants to extract as much value from the user as possible" hat.
- Write down all the ways that you can make money from the user (or the user's data), while not violating the letter of the privacy policy.
    - You earn bonus points for being evil.

And let's not forget . . .

- Use Free Software!
- Free software respects your freedom.
- Free software respects your privacy.
- It's hard to backdoor software when the source code is public.

Thank You

(for supporting free software)