Practical
Everyday
Counter-Surveillance

Slides, notes, links, and resources available at

https://github.com/Bard-EH/PECS

Step 1:
Understanding Your Security Landscape With Threat Modeling

Threat Model Questions

1) What am I trying to protect?
2) Who am I trying to protect it from?
3) How likely is it that I will need to protect it?
4) How bad will things be if I fail to protect it?
5) How much trouble am I willing to go through?

Example: Leaving the apartment

1) What am I trying to protect?

➔ The stuff in my apartment

➔ My cat from getting out

Example: Leaving the apartment

2) Who am I trying to protect it from?

➔ Thieves

➔ My cat (who can open unlocked doors)

Example: Leaving the apartment

3) How likely is it that I will need to protect it?

➔In Red Hook? Not terribly likely, but possible

➔In NYC? Somewhat more possible

Example: Leaving the apartment

4) How bad will things be if I fail to protect it?

➔ I guess it depends on how important your stuff is

Example: Leaving the apartment

5) How much trouble am I willing to go through?

- ➔ Close the door
- ➔ Lock the door
- ➔ Bars on windows
- ➔ Live in a gated community with security guards
- ➔ Move to Mars

Practice makes proficient.

Analyze your decisions
Reverse-analyze the decisions of others

“What is that surveillance camera doing there?”
“Why is that door so big and heavy?”

“Why is that bench shaped like that?”

Targeted or Mass Surveillance

Targeted

- It's when **THEY** are after **you**!
- Most useful framework:
- "Mossad" / "Not Mossad"

Targeted: Not Mossad

- How do you defend your email from hackers?
  - → Strong, unique passwords
  - → Two-factor authentication
  - → Don't be dumb

Targeted: Not Mossad

- How do you defend your email from your creepy ex?
  - ➔ Strong, unique passwords
  - ➔ Two-factor authentication
  - ➔ Maybe date better people

Targeted: Mossad, NSA, FBI, GRU…

- How do you, a regular person, reliably defend against a persistent, intelligent, aggressive adversary with effectively unlimited funding, resources and time, who is dedicated to breaking down any defenses you raise against them?

You Don’t

Mass Surveillance:
You're Already A Target

Step 2:
Understanding Where You're At

Taking Stock

- Look at every app on your smartphone, every app on your computer, every website you frequent, and ask:

1) What does it know about me?
2) Who does it tell what it knows about me?
3) Do I use this? Do I *really need* to use this?
4) Are there alternatives?

Step 3:
Reduce your Vulnerability Surface

Reducing Your Vulnerability

- Wipe your histories – past is prologue
- Back up vital data – download those Google drive files, stick them on a USB drive
- Delete what you don't need and/or don't use
- Seriously consider alternatives to Facebook, Google, and Apple products

- At the very least, understand what they know about you (and who knows what they know)

Step 4:
Proactive Security

The Bit Where I Talk About Tools

- Browser extensions
  - µBlock Origin ←Blocks most ads
  - Privacy Badger ← Blocks most trackers
  - HTTPS Everywhere ← Keeps your info safe in between you and the server

The Bit Where I Talk About Tools

- Password managers: Pick one, use it
  - Lastpass ← Free, web-based sync
  - 1password ← Not free, web-based sync
  - KeePass ← Free, manual sync

- Device encryption
  - Apple & Android phones: Easy
  - Computers: somewhat harder

The Bit Where I Talk About Tools

- Chat/Communications
  - Signal ←Just use it
  - VPN ← Be careful! Probably don't!
  - Tor ← Also be careful!
  - PGP/GPG ←Eughhhh

Closing thoughts

- "Security is a process, not a product" – Bruce S.
- Guarantee one of these tools will have a major flaw discovered within a year.
- Keep your head up, be proactive, read the tech news, keep everything up-to-date
- Research a new tool before you use it

Slides, notes, and resources available at
https://github.com/Bard-EH/PECS

My email
gsablosky@bard.edu

My personal email
sabo@lattid.com

Practical
Everyday
Counter-Surveillance

Say your name, attack own credibility, feel free to jump in

Hands: If you've self-censored; if you're expecting to self-censor

So what can you do to help fix that? No one knows, because no one knows what's coming next policy-wise

T wants to get "tough on cyber", but "the security aspect of the cyber is very very tough". and his 10-yr-old is good with computers.

Goal is not to (just) give you a list of tools, but a framework to recognize, analyze and deconstruct systems of security & surveillance in your daily lives;
Impart basic principles of mitigation (crypto, covering tracks)

- Everything is available online at this url
- links to references and tools

Step 1:
Understanding Your Security Landscape With Threat Modeling

When thinking about issues of security, privacy, and counter-surveillance, it's really vital to have a clear picture of what you're up against. To do that, we need to create a threat model.

A "threat model" is a systemic analysis of potential threats to something thing you want to defend. The process of building one is a way of thinking through the possibly-daunting problems of security in a repeatable, general way.

One really useful set of questions for building threat models comes from the EFF, basically the ACLU for computer nerds.

Threat Model Questions

1) What am I trying to protect?
2) Who am I trying to protect it from?
3) How likely is it that I will need to protect it?
4) How bad will things be if I fail to protect it?
5) How much trouble am I willing to go through?

These questions offer a basic rubric for evaluating threats to personal security, physical security, information security, national security...all the securities.

Some of you may be more familiar with thinking about things in these terms than others. But everyone does some form of this evaluative process in their daily lives, if not in this rigorous a fashion

There are other ways to do threat modeling, also. This is just one rubric.

Example: Leaving the apartment

1) What am I trying to protect?
   - ➔ The stuff in my apartment
   - ➔ My cat from getting out

Let’s run through one quick example of applying this framework. It’s a normal day, you’re heading to class or work, and you’re leaving your dorm or apartment.

Example: Leaving the apartment

2) Who am I trying to protect it from?

➔ Thieves

➔ My cat (who can open unlocked doors)

Example: Leaving the apartment

3) How likely is it that I will need to protect it?
   - ➔In Red Hook? Not terribly likely, but possible
   - ➔In NYC? Somewhat more possible

I had to remind my landlord to give me the keys to my apartment, since he wasn't used to keeping things locked.

Example: Leaving the apartment

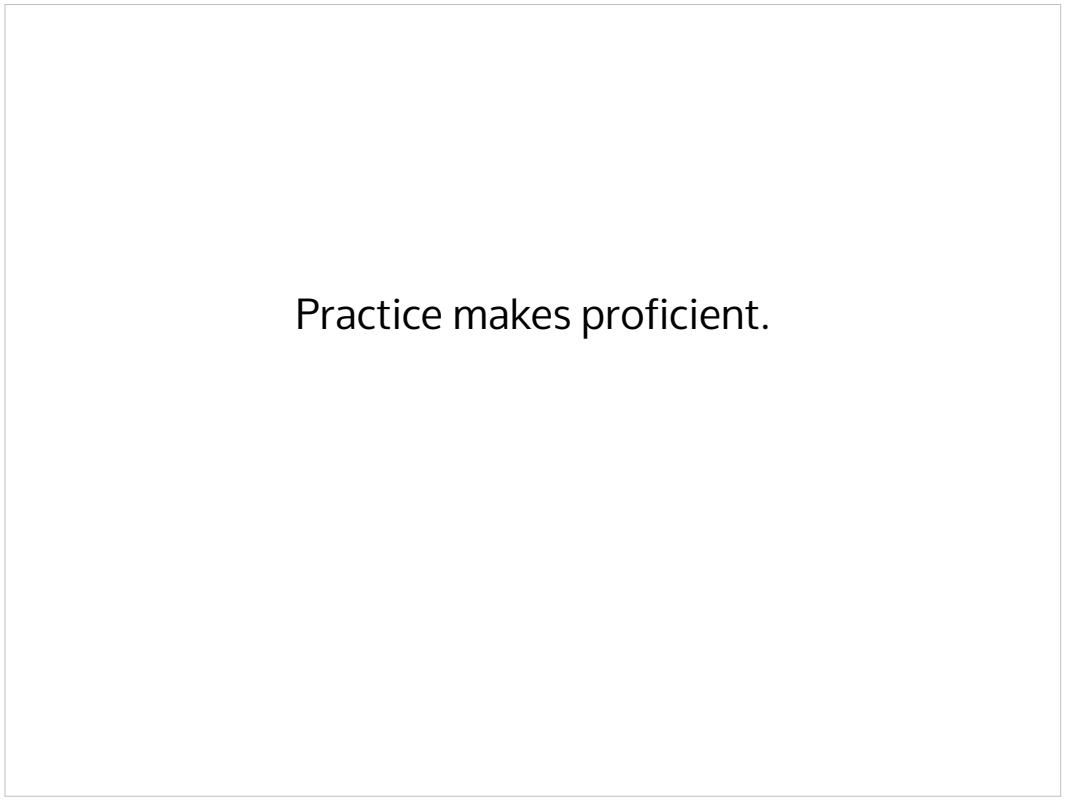
4) How bad will things be if I fail to protect it?

➔ I guess it depends on how important your stuff is

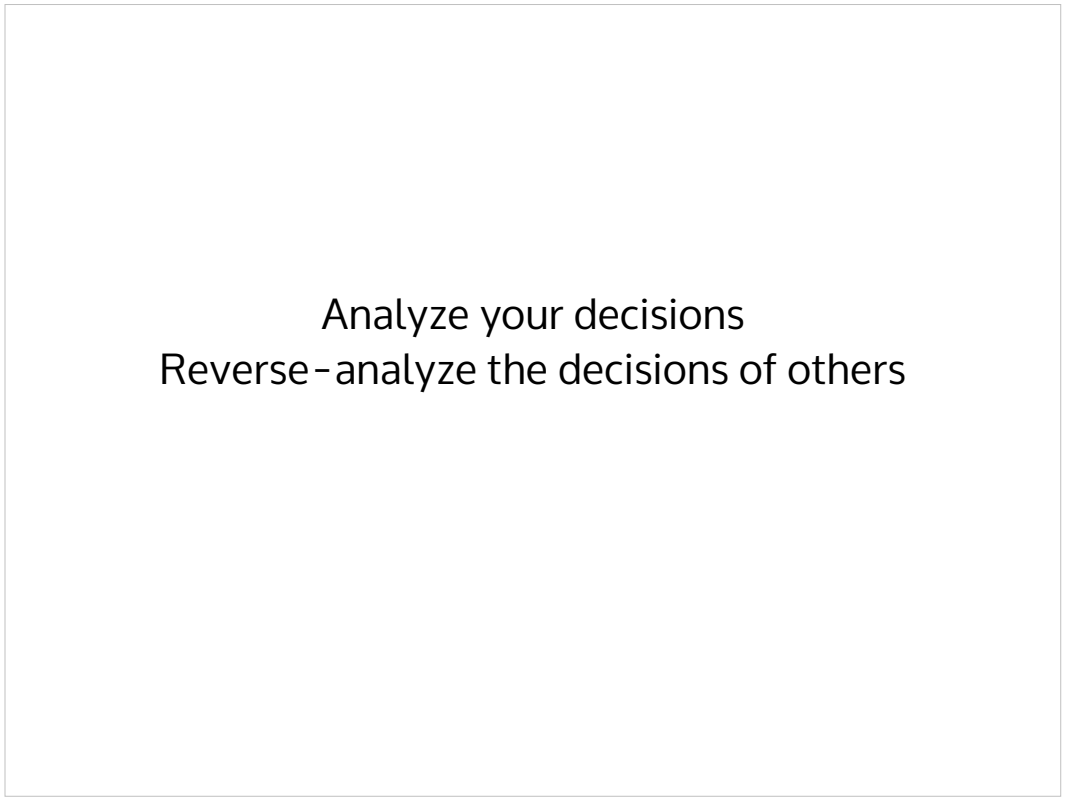
Example: Leaving the apartment

5) How much trouble am I willing to go through?

- ➔ Close the door
- ➔ Lock the door
- ➔ Bars on windows
- ➔ Live in a gated community with security guards
- ➔ Move to Mars



Nobody gets this stuff right 100% of the time, but the more you think about and understand threats in a systemic way, the easier and more reflexive it becomes.



The next time you do something out of habit, try thinking of it in terms of threats and protecting yourself from threats. (This may not always work.)

This doesn’t have to be a scary, paranoid thing: do it with brushing your teeth, walking your dog, etc! The important thing is to run through the questions and be aware of the process.

Likewise, look at the world around you, and try to reverse-analyze it from a security perspective

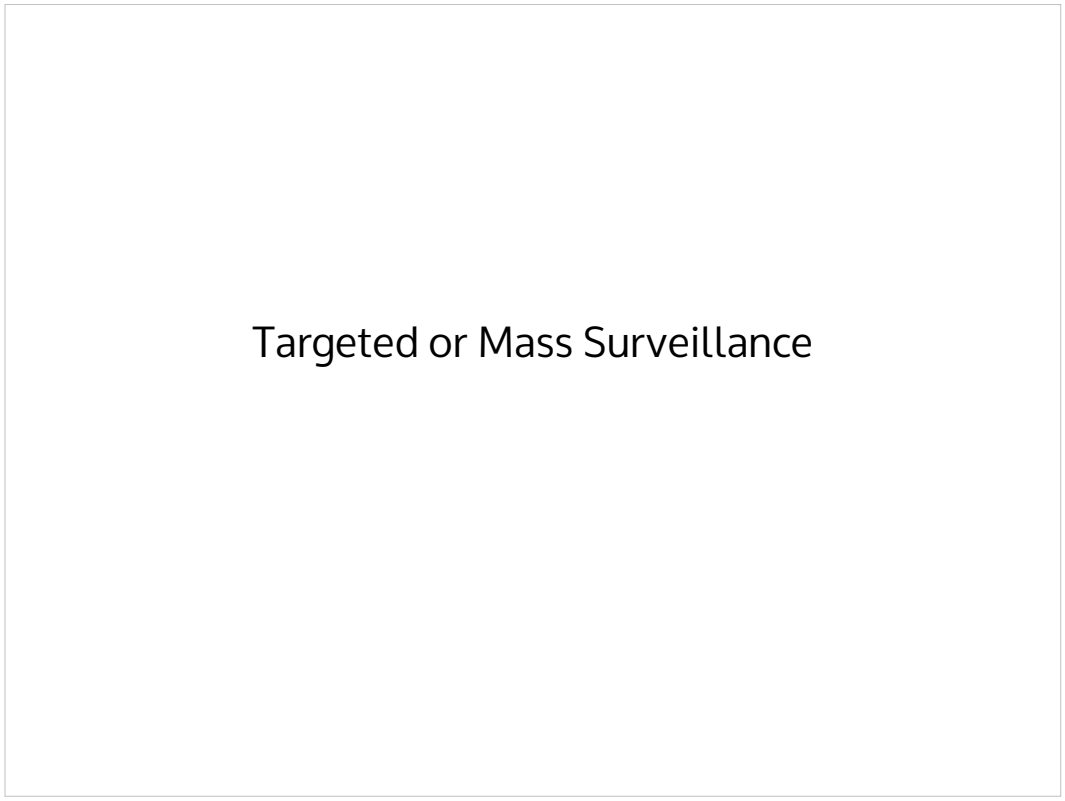
"What is that surveillance camera doing there?"
"Why is that door so big and heavy?"

Think about both the obvious signs of surveillance/security, and the not-so-obvious ones...

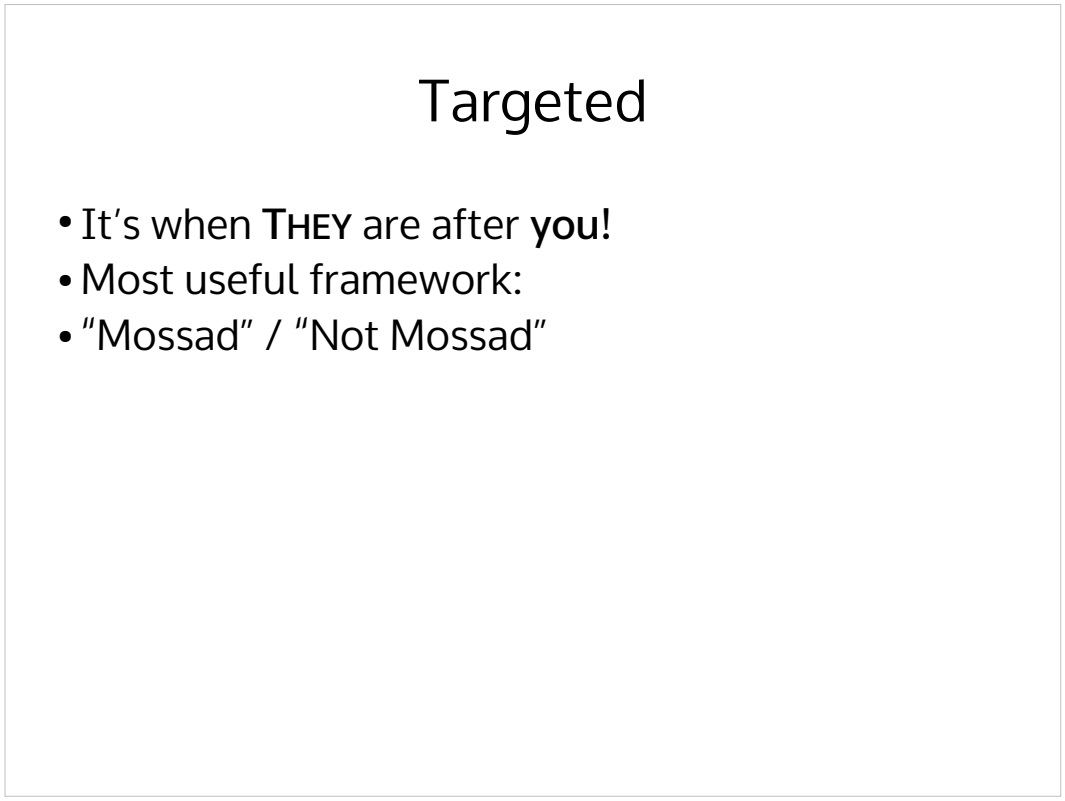
"Why is that bench shaped like that?"

This is called a Camden bench. It's a bench designed defensively, a bench designed with a threat model in mind. You can sit on it...and not much else.

If you are a certain kind of person and want to "protect" a certain notion of public space, this is the bench you want. You can't sleep on it, you can't sit side-by-side with someone, you can't skateboard on it, you can't hide anything under it, it's resistant to graffiti, you don't need to bolt it to anything since it's so heavy...and it doubles as a counter-terrorism roadblock.



Now we come to the question of surveillance. When you try to build threat models for all the different types of surveillance, you can divide the world into two broad categories: targeted or mass surveillance.



Targeted surveillance is when Someone is trying to spy or get information on YOU – as an individual person. The most useful way to understand targeted threats really breaks down into a binary based on the relative power and capabilities of the attacker.

which for me was clearly described in an essay by a researcher for Microsoft named James Mickens on how computer security people talk about security:

Am I up against one of the most cunning and resourceful intelligence agencies in the world, or some random jerk?

Is it Mossad, or Not-Mossad?

Targeted: Not Mossad

- How do you defend your email from hackers?
  - Strong, unique passwords
  - Two-factor authentication
  - Don't be dumb

Hackers, at least the sort who want to use your email to steal your netflix password and spam retireees about herbal viagra, are Not Mossad.

It's pretty easy to stymie that sort of hacker. Use a good password, set up two-factor authentication – where you scan a code into an app on your phone, or get texted a code, that you have to enter when you login from a new computer. Google supports it, now Bard Mail supports it, Facebook supports it...you really should use it if you can.

Also, don't click on any links for herbal viagra.

Targeted: Not Mossad

- How do you defend your email from your creepy ex?
  - → Strong, unique passwords
  - → Two-factor authentication
  - → Maybe date better people

Your creepy ex is (hopefully) Not Mossad.

The steps you take here are basically the same. Strong passwords, two-factor authentication, maybe date better people.

Targeted: Mossad, NSA, FBI, GRU…

- How do you, a regular person, reliably defend against a persistent, intelligent, aggressive adversary with effectively unlimited funding, resources and time, who is dedicated to breaking down any defenses you raise against them?

So now let’s check out the other side of this coin.

You can certainly make it harder for them to get you! Encrypt everything, drop off the internet, move to Belize, grow a beard, then shave it off, wear aviators...but if they want it bad enough, they will end up getting what they want, in all likelihood.

The best way to beat targeted surveillance is to never make yourself a target in the first place. Either by being very boring and complacent, or by being smart about how you go about being exciting and challenging.

Mass Surveillance:
You're Already A Target

Which brings us to Mass Surveillance. You're already a target, you probably know that, but it's possible to make things more difficult for the people doing the mass-surveilling

Mass surveillance consists of government programs that monitor information indiscriminately, corporations that make money off of your personal info, and programs that bridge that gap, such as PRISM (where 90% of the NSA's data comes from)

Avoiding mass surveillance is an end unto itself, but it will also reduce the chances of you – and those you interact with! – becoming subject to targeted surveillance.

Step 2:
Understanding Where You're At

So now that we know how to analyze threats, and the general sorts of threats you might encounter, let's move on to taking stock of where you're at in the world of mass surveillance.

Unfortunately I can only offer general advice for steps you may want to take, since everyone is a unique and special snowflake. But if you have specific questions or concerns, again, feel free to ask or get in touch with me later

Taking Stock

- Look at every app on your smartphone, every app on your computer, every website you frequent, and ask:

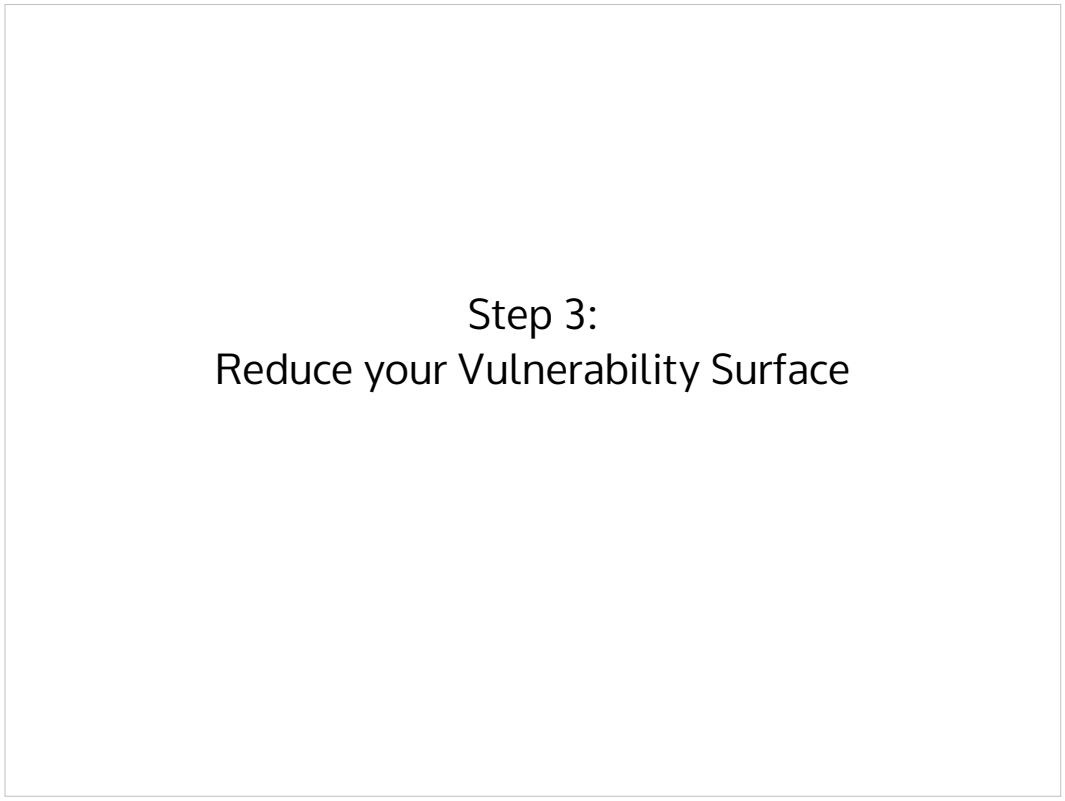
1) What does it know about me?
2) Who does it tell what it knows about me?
3) Do I use this? Do I *really need* to use this?
4) Are there alternatives?

The main business model of the internet is driven by advertising. Advertising becomes more valuable if it's targeted to people who might click on the ad.

Frinstance, I will never click on an ad for horse-racing stuff, since I don't race horses and have no interest in horse racing.

Unfortunately, that basically means that every advertising company is deeply invested in building as reliable and comprehensive of a profile on you as possible.

The Snowden leaks, specifically the PRISM program, demonstrated how those databases can be shared, forcibly or willingly, with government agencies



With that understanding of how you use technology, and how it interacts with systems of corporate and government surveillance, the next step is to minimize what you feed into these systems.

Reducing Your Vulnerability

- Wipe your histories – past is prologue
- Back up vital data – download those Google drive files, stick them on a USB drive
- Delete what you don't need and/or don't use
- Seriously consider alternatives to Facebook, Google, and Apple products

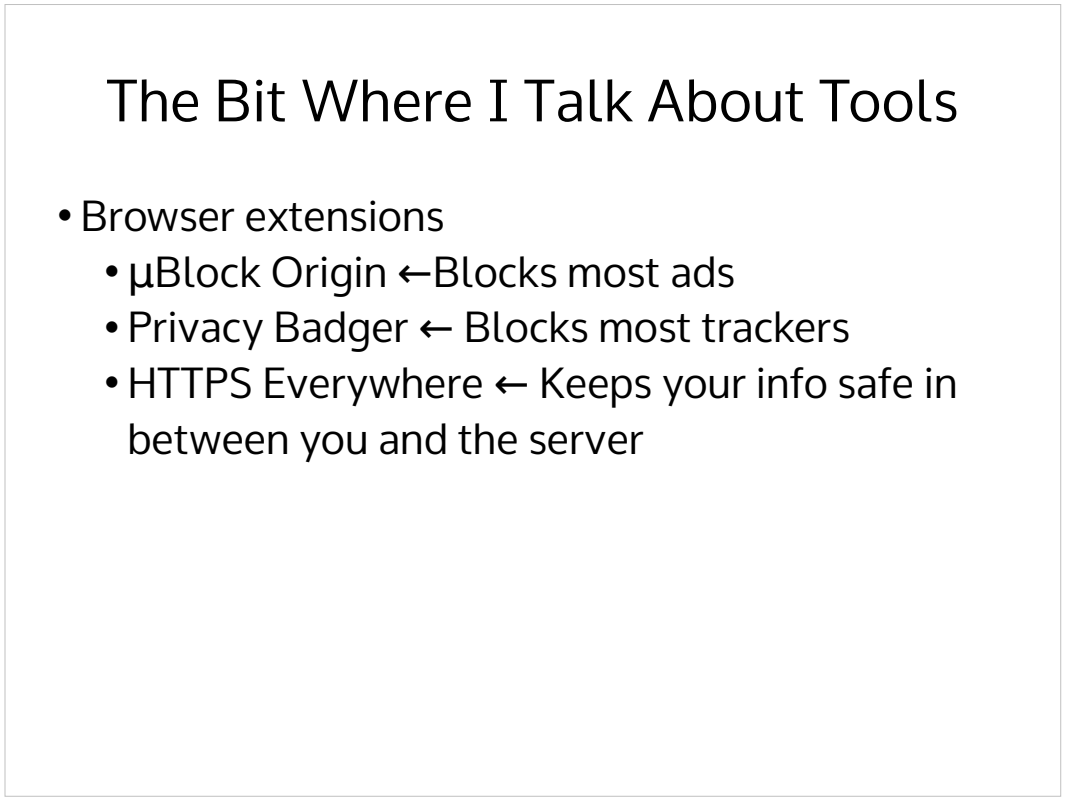
- At the very least, understand what they know about you (and who knows what they know)

If you go to the github page, I've put a bunch of links to the more important and somewhat hidden areas of Facebook and Google that control privacy settings, as well as how those companies see you.

Step 4:
Proactive Security

Now that you're feeding as little as possible into the surveillance-industrial complex, I'd like to recommend or mention just a few tools and services that actively resist surveillance. Several of these tools rely on or enable the use of encryption.

Word of caution: Encryption is tricky to do right. It sits at the intersection of math and engineering in a way that means people who are experts in either but not in both often get it wrong. So when you see some new product or service that offers encryption as a selling point, be critical. Search around, read reviews, look for recommendations...if you see a lot of critical coverage, or a lack of a good cryptographic analysis don't use it. I know this is a big ask, but this is the way the world is.



There are a few browser extensions for Firefox and Chrome that work out of the box and will improve your piracy.

If you are using any ad-blocker other than ublock origin, switch. It's more performant and, unlike old-school AdblockPlus, has not yet sold out.

Privacy badger is a project by the EFF that blocks some ads, and most social network trackers. These nasty buggers track you whether or not you've got a facebook/google account

HTTPS Everywhere prevents eavesdroppers in between you and the server you're communicating with from reading your communications. It's by no means foolproof, but it's strictly speaking better than the alternative.

The Bit Where I Talk About Tools

- Password managers: Pick one, use it
  - Lastpass ← Free, web-based sync
  - 1password ← Not free, web-based sync
  - KeePass ← Free, manual sync

- Device encryption
  - Apple & Android phones: Easy
  - Computers: somewhat harder

The best passwords are also the hardest to remember. Just make them really long and really random. Don't worry about remembering it. If any of you are familiar with the correct-horse-battery-staple rule from XKCD…those have been weak for a really long time. Your vocabulary is not as big as you think, and password-crackers adapted to them years ago.

Full-disk encryption is built into most modern mobile and computer operating systems. Use it if you can. Use a long, strong passwor.d

The Bit Where I Talk About Tools

- Chat/Communications
  - Signal ←Just use it
  - VPN ← Be careful! Probably don't!
  - Tor ← Also be careful!
  - PGP/GPG ←Eughhhh

As far as chat goes, whatever you're using to text, you should probably switch to Signal. If you only do one thing I recommend, use Signal and convince your friends to use Signal. It's got great, audited encryption, it's easy to use for a crypto app, and it will keep your communications secure. (Cover it at the end)

The other things on this slide...use only if you're really positive that you need them, and if you're positive you know how to use them. I can't give them a blanket recommendation. Look on the github for my reasoning on that

Closing thoughts

- "Security is a process, not a product" – Bruce S.
- Guarantee one of these tools will have a major flaw discovered within a year.
- Keep your head up, be proactive, read the tech news, keep everything up-to-date
- Research a new tool before you use it

If you take away one thing from this workshop, let it be this: no tool is perfect. Don't think in terms of tools. There's a great cryptographer named Bruce Schneier, and he has this saying that "security is a process, not a product". Privacy is a process, C-S is a process, they are not products.

Every computer program has bugs. Some of these bugs, even in open, well-audited codebases, can cause breaks in their security.

Analyze your security. Analyze threats. Read what the surveillance state is up to now. Be critical

Slides, notes, and resources available at
https://github.com/Bard-EH/PECS

My email
gsablosky@bard.edu

My personal email
sabo@lattid.com

- Thx