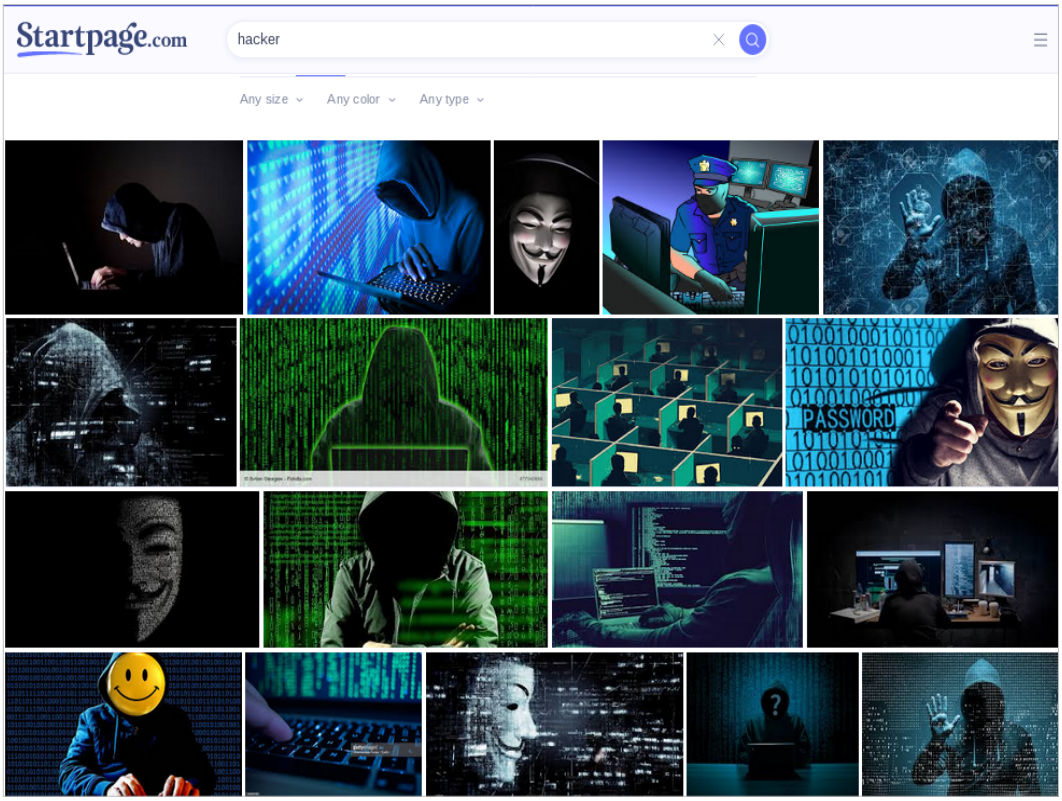
Small mention of interesting things

- Assignment due tomorrow by 11:59 PM (MST). No late penalty!
- TCEs

Today will review the semester.

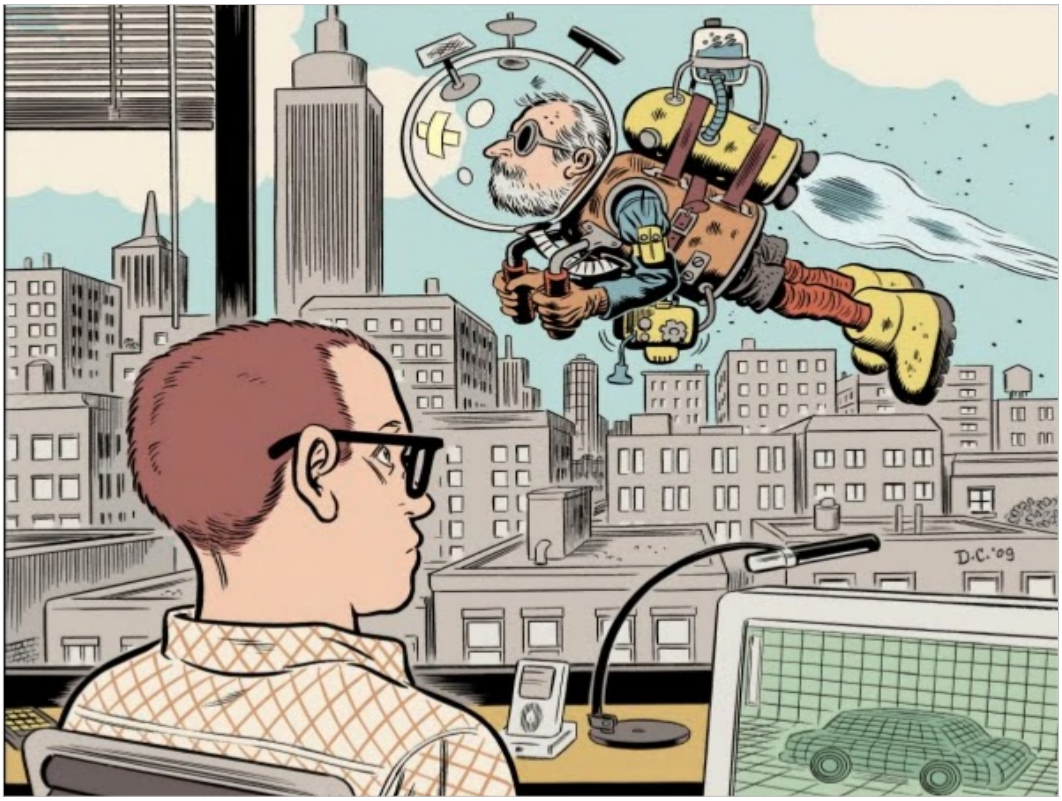
A basic appreciation for what you don’t know, and how to fix that, is useful. So is recognizing bullshit (technical term from Frankfurt, see ‘Cybercrud’ in recent assignment) and more general pretentiousness.



it’s tricky to stay grounded when learning about privacy and security technology. There’s a lot of hype, and things related to hype.

That’s a good reason to make fun of all that stuff, and keep straight in your head that (a) you don’t know much, but (b) there’s a lot of interesting stuff to learn, and (c) you are capable of knowing more, and doing cool stuff with that knowledge

Haha, only serious



We studied computational privacy technologies in this course.

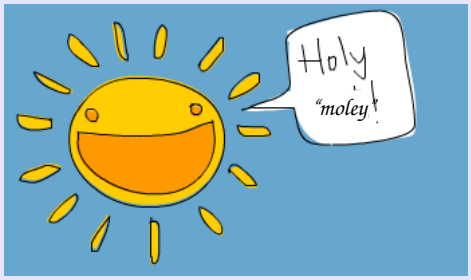
Stopping with creating technology would be incomplete: the other side of studying privacy technologies is understanding the context of those technologies, including ultimately the ability to identify where an emerging problem may lie, and what approach might be best to mitigate it.

Let’s start with some technologies

COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

Every darn thing

- recognize security problems
- set up a server for your own purposes
- set up an onion service
- countermeasures to standoff biometry
- building trust rationally
- learn a cryptographic primitive that is new to you, and implement it



6

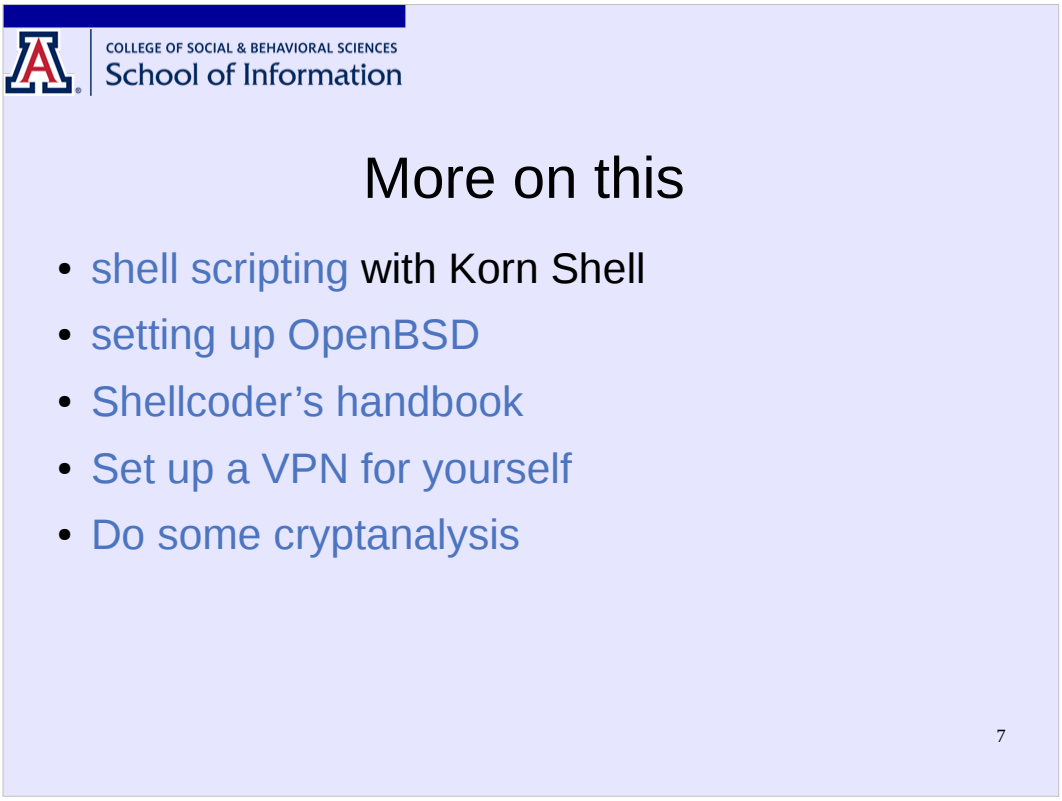
Security problems:

- find setuid binaries
- test for password weakness
- test for permissions mistakes
- observe your logs

- “Set up a server”: Do it yourself. That is a powerful general thing about privacy technology. Doing it yourself helps you to make sure that your technology does what you want, and doesn’t betray you (which most of it does, to some degree or other).

Building trust.

- using WoT as a conceptual exercise. Thinking about PKIs and certificate transparency as trust-building
- Crypto learning with RSA and DH



Ksh is the default shell in OpenBSD. OpenBSD is good for learning about security: that is the distribution's focus. It is also good for learning more generally: their man documentation is among the best I've found---this link is to "afterboot," which gives you a checklist of things to do after you've first installed OpenBSD. Follow it, and learn about everything you're doing (links to the man pages are included, or you can do it in the man page on your system itself with $ man afterboot).

Shellcoding is an excellent avenue into a deeper understanding of a lot of stuff: memory management is the prime example, but much more besides! You have fun trying to elevate priviledges, and become an expert without feeling it. This book is a classic.

Set up a VPN. People will sometimes be glib about VPNs, but think: what is the threat model, and how is it different from (e.g.) Tor's? (Consider privacy from your ISP. Consider rotating VPN servers with an automated configuration script).This link is to the community docs---there are other docs that are not as useful.

An attitude of blithe disregard to privacy is common, but you need only look at the size of the organizations that exploit personal data to see that most people are misled: their data is being used, and not always to serve their interests.

Google has 60 services that collect data from you in a huge variety of contexts: making choices about your physical environment at home (Nest, Echo), where you choose to go (Google Maps), what shows you choose to watch (Youtube, Chromecast), what you choose to take/store pictures of (Google Photos), the books you are interested in (Google Books), the general pattern of websites of all types that you visit (Google Analytics, Chrome Browser), who you share documents with (Google Docs).

Having taken this class, you should be able to recognize privacy problems with this kind of thing, with a little thought.


Maciej Cegłowski, Haunted by Data

A similar point can be made about government surveillance. And here we have learned about some history in other countries (the Stasi), and in this country (COINTELPRO, leading to the Church committee)

“the committee noted, every president from Franklin Roosevelt to Richard Nixon improperly used government surveillance to obtain information about critics and political opponents.”

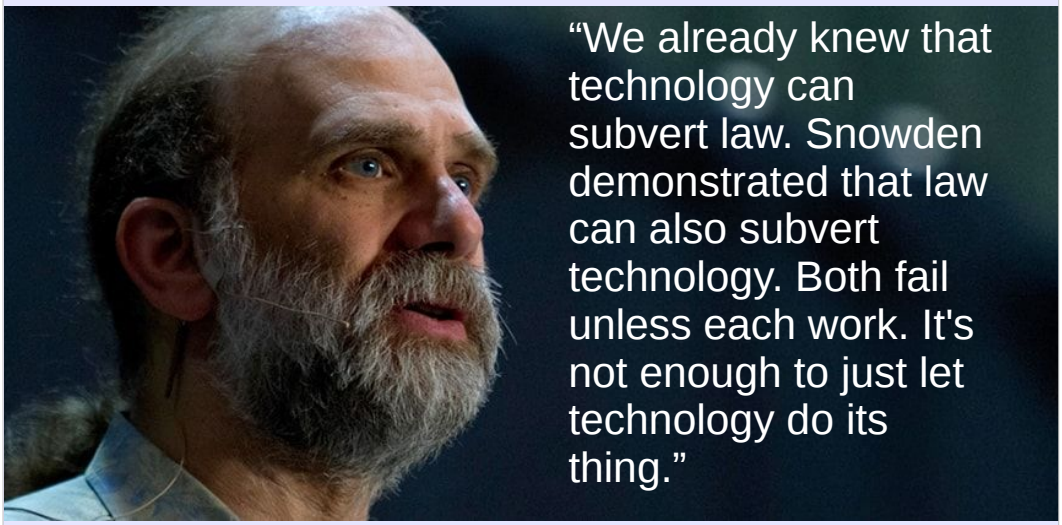
“While the declared purposes of these programs were to protect the "national security" or prevent violence, Bureau witnesses admit that many of the targets were nonviolent and most had no connections with a foreign power. Indeed, nonviolent organizations and individuals were targeted because the Bureau believed they represented a "potential" for violence—and nonviolent citizens who were against the war in Vietnam were targeted because they gave "aid and comfort" to violent demonstrators by lending respectability to their cause..”

-- The Church Committee

In more recent news, we have seen the Espionage Act, which was enacted during wartime, used in a discretionary way to control whistleblowers.

Remember this quote from Hal Abelson?

COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

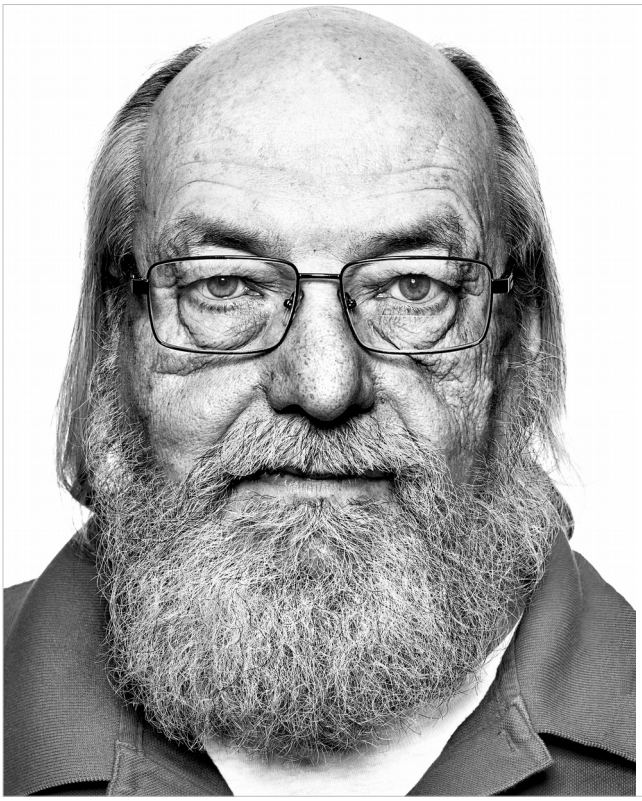


12

Abelson’s quote lead us to ask, “who will protect us from the dark arts?”

The answer involves policy and technology, or technology in context. (Schneier quote is a little misleading: explain a little).

Privacy technology can have various relationships to their social context. Here it helps to compare research on privacy technologies for control and for confidentiality separately.



The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me). No amount of source-level verification or scrutiny will protect you from using untrusted code.

Ken Thompson, ACM Turing Award Speech, “Reflections on Trusting Trust”

Privacy as control requires distinguishing the trustworthy from the untrustworthy, and trying to trust only the right entities.

Here trust is a social thing, built up through networks of previously established relationships, or by technologies of reputation tracking or other kinds of transparency.

If not source-level verification or scrutiny, then what? we might ask...

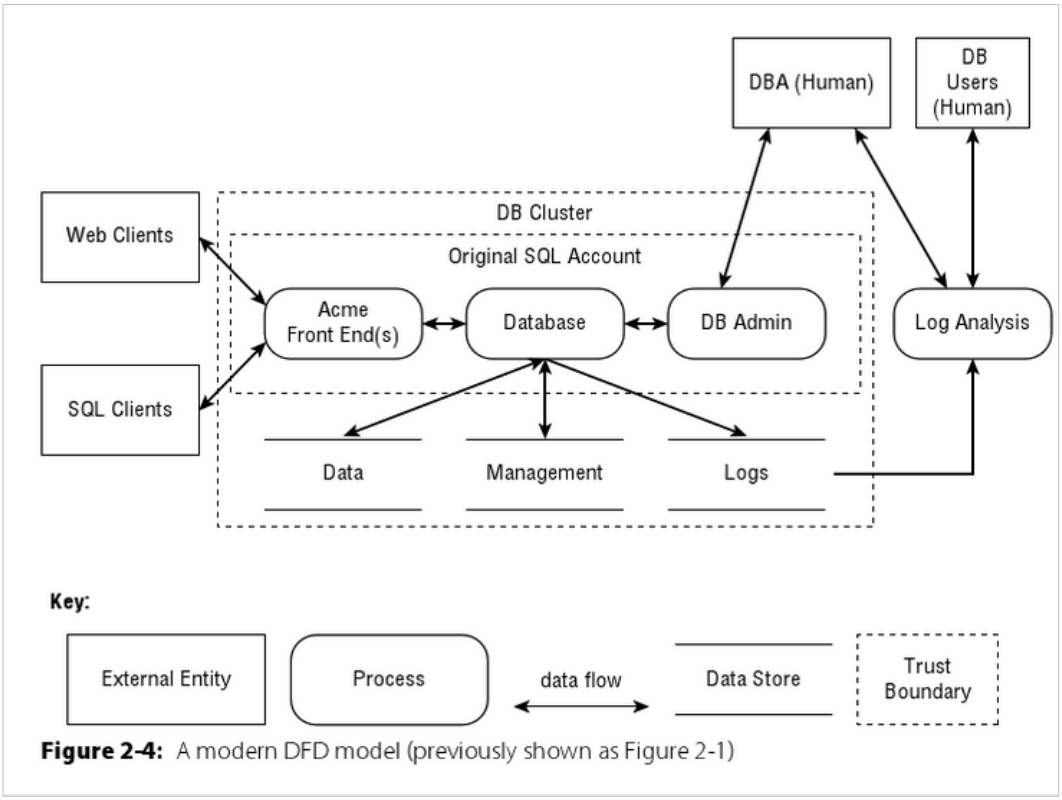
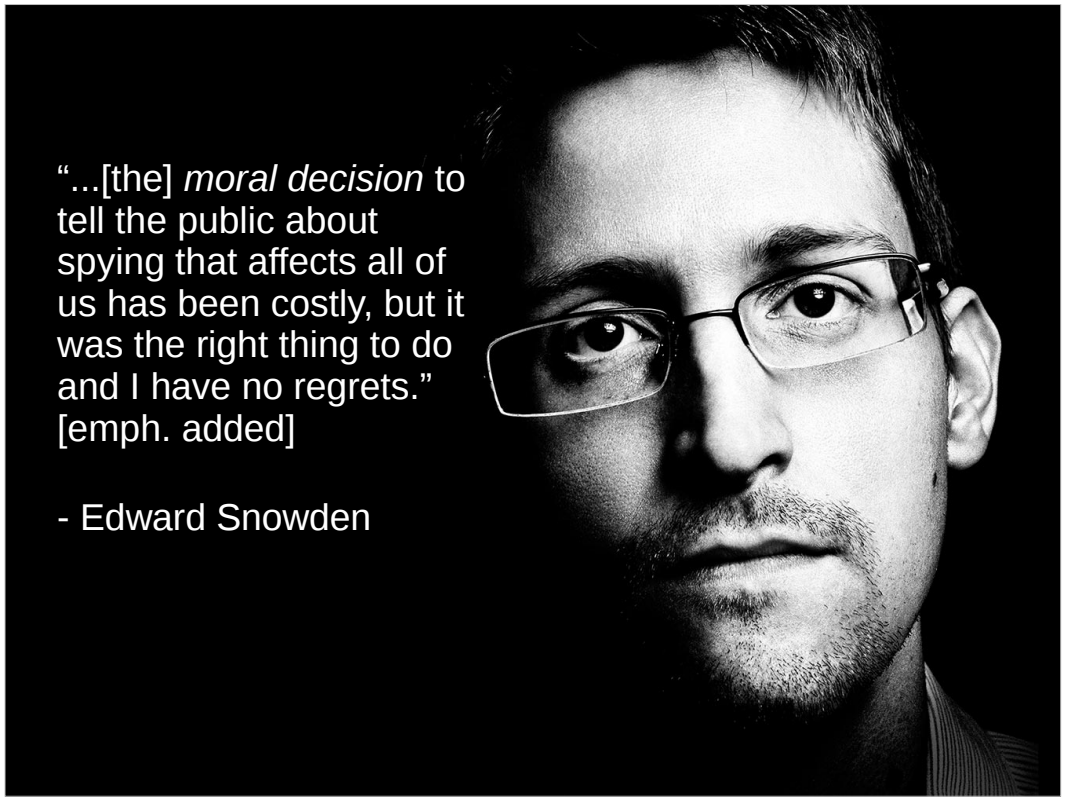


Figure 2-4: A modern DFD model (previously shown as Figure 2-1)

We have seen another approach to privacy technology several times, where cryptography is used to be more conservative: it gives up on distinguishing, and just tries to minimize trust. The picture of trust here is from the security community: in threat modeling a trusted system is one whose failure would break the security properties of the system (Anderson, Shostack on this).

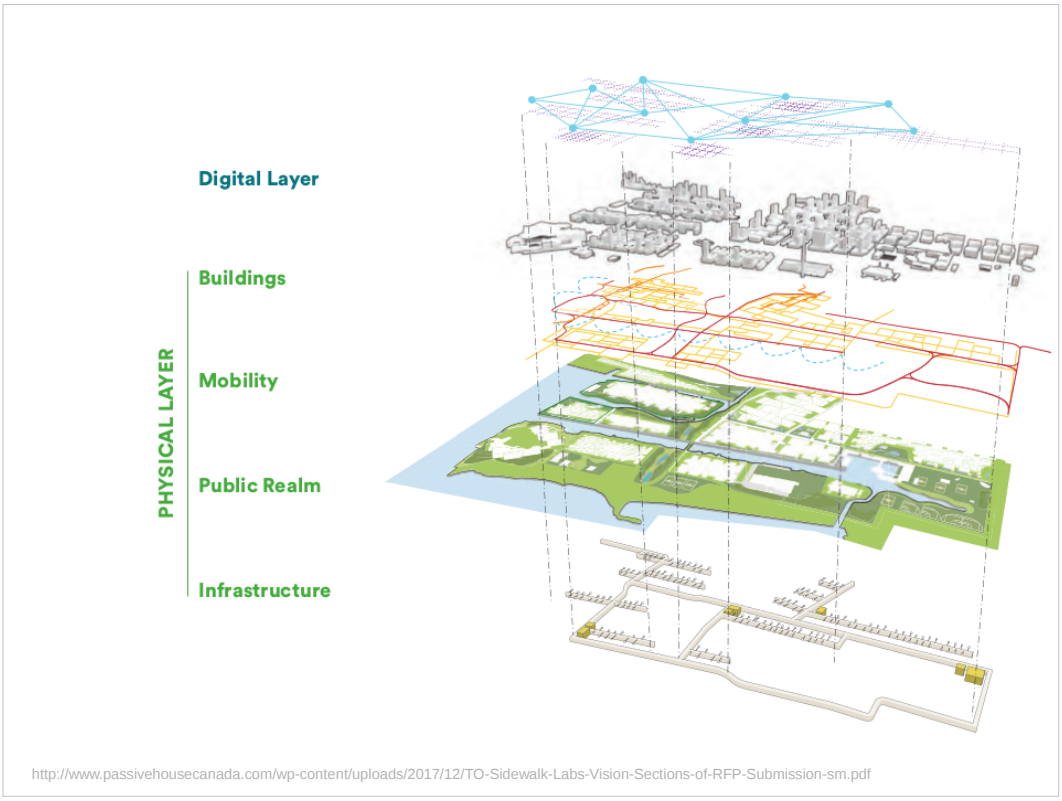
Minimizing false positives is a security mindset that is not without cost. Privacy technologies should balance false positives against false negatives with regard to trust relationships, to avoid becoming an isolated crackpot.



Privacy a normative, ethical component as well, as we've seen. That is the context in which we evaluated Snowden's revelations as an act of civil disobedience.

Snowden explained the deliberations leading to his decision to act. What virtues of character were evident in his actions, if any? Should being properly disposed with respect to privacy itself be understood as a virtue (akin to being properly disposed with respect to the environment, which Hursthouse argued for)?

Here technologies like SecureDrop can be seen as important for their role in supporting the ethical decisions of whistleblowers. Knowing how to use them is part of the practical wisdom required to be a person who is able to act ethically to protect the privacy of others.



http://www.passivehousecanada.com/wp-content/uploads/2017/12/TO-Sidewalk-Labs-Vision-Sections-of-RFP-Submission-sm.pdf

Automated systems capable of violating privacy may be used to build a future that we don't want.

On the horizon: an entire portion of a city given to Google (Sidewalk Labs in Toronto: "The genesis of the thinking for Sidewalk Labs came from Google's founders getting excited thinking of 'all the things you could do if someone would just give us a city and put us in charge,'" Eric Schmidt). This takes Google firmly into the realm of layer 8 issues (since Google glass didn't work out). Ann Cavoukian has resigned from this project in protest over the collection and sharing of data that is now planned.

As Dan Geer said: "If privacy both as impossible-to-observe and impossible-to-identify is dead, then what might be an alternative? If you're an optimist or an apparatchik, your answer will tend toward rules of procedure administered by a government you trust or control. If you're a pessimist or a hacker/maker, your answer will tend toward the operational, and your definition of a state of privacy will be mine: the effective capacity to misrepresent yourself."

Despite the admirably heroic feeling here, we've seen that one need not always be entirely of either camp, but be a sophisticated contributor to both---for example, by making a business case for infrastructure providing privacy protection in order to prevent costly disclosures. This is what privacy in context is all about.

Not everyone has given it a little thought or taken a class on privacy, so you should help to provide perspective on privacy issues like this, and where they may lead. The progression towards a problem is not always clearly marked with bad developments (although we do sometimes see blockbuster disclosures) ---the more pernicious problem, which justifies your activity as privacy-informed, is mining for low-grade ore rather than big gold nuggets---i.e., the accumulation of lots of innocuous-seeming data collected across a variety of contexts where such collection makes sense. We saw this in the last lecture, and it resonates with a quote from the first lecture:

“The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate recordkeeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.”
Privacy Protection Study Commission, Personal Privacy in an Information Society, established by the Privacy Act of 1974.

Privacy is a broad social issue, not a narrowly narcissistic one. As much as people like to joke about it, in the age we live in, it is serious---disregarding it is bad not only for the individual, but for the broader society in which she lives.

Privacy is a fundamental civil liberty, underlying fundamental freedoms to thought, speech, bodily integrity, property, association, and more.

Technology, especially the computer technology we've focused on in this class, can be used not only to capitalize on increased information asymmetry by making money and increasing the concentration of power, but to enforce the protection of the vulnerable, to build business and personal relationships on a foundation of respect for privacy, and more generally preserve social values that otherwise would go undefended against "the dark arts."

I hope you will go on to contribute to the creation of technologies for privacy enhancement suited to their context in this spirit (and that you'll tell me when you do)!