1 Privacy

This is an informal workshop, given at the 2015 May First/People Link member's conference

1.1 What is Privacy?

You can find many definitions for the word "privacy". A dictionary will say something like "The state of being private; the state of not being seen by others." Judge Louis Brandeis called it "the right to be left alone". Dan Geer called it "having the ability to misrepresent oneself." The UK's CCTV program used the motto "If you've got nothing to hide, you've got nothing to fear". I'm not very fond of these last two: they imply that privacy's usefulness is limited to people who wish to misrepresent themselves, or having something to hide. That's simply not the case.

I'd like to talk about privacy as it relates to communications – how we talk and interact with one another. In the physical, face to face world, this is very easy to understand. If you can a friend are having a loud roudy conversation on the bus, then the whole bus is going to hear it. Both of you knew that, and probably didn't care too much at the time. On the other hand, if you pull your friend aside into a quiet corner of the room, you're not expecting anyone else to hear what you're taking about. And if someone is creeping up and trying to listen, one of you will probably notice.

Communications in the digital world are very different. Even solo interactions are very different. For example, people have very personal relationships with their phones, with video streaming services, and with internet search engines. Years ago, Netflix and AOL released large collections of "anonymized" user searches; in both cases, people were able to de-anonymize some of the data. Google recently announced that it's been recording and retaining voice queries. Even if companies don't release this kind of information to the public, lots of people in the company have access to it. As do the employees of other organizations they share data with, or sell data to. Your personal relationship with your phone, or a third party service probably involves a lot more people than you realize.

1.2 Risk Management

When we get into digital communications, privacy really turns into a game of information security, and your ability to have some control over how information about you is used.

Information security falls under the broad heading of risk management. Risk management is about as exciting as buying insurance (which itself is a form of risk management). The basic idea is that we start with something bad that might happen. Risk management is whatever you do to prevent that bad thing from happening, or to make it less bad when it eventually happens. I've already mentioned insurance. A couple of other examples:

- locking your door
- wearing a bicycle helment
- looking both ways when you cross the street

This sort of thing happens on a continuum, and it involves a balancing act. Having two locks on your front door is safer than having one, and having fifteen locks on your door is safer than having two. But who wants to deal with fifteen locks? It really comes down to what you perceive as a risk, and how much inconvenience you're willing to tolerate in order to mitigate it. That's security in a nutshell, and it's different for everyone.

In terms of communications privacy, what do you guys see as risks?

1.3 Resources

I expect that much of this discussion will be driven by folk's perceived risks. However, here are some general resources.

- EFF's surveillance Self-Defense guide. `https://ssd.eff.org/`
- PRISM Break. `https://prism-break.org/en/`
- Guardian Project. `https://guardianproject.info/`
- Email Self-Defense. `https://emailselfdefense.fsf.org/`
- A large collection of presentations from the Tor Project. `https://media.torproject.org/outreach-material/presentations/`
- GnuPG (`https://gnupg.org/`), GPG4Win (`http://www.gpg4win.org/`), GPGTools (`https://gpgtools.org/`)
- Cryptoparty. `https://www.cryptoparty.in/`