

# CSE 303: Concepts and Tools for Software Development

## Discussion on the Ethics of Digital Privacy

27 April 2005

### Issues for Discussion

Computer technology has changed our lives by making it easy to store, access, and process enormous amounts of data. This power enables many good things, but it can also enable bad things, such as providing information to entities that we wish did not have it. That is, technology has raised new *privacy* issues.

#### Technology Areas:

- Web browsing:
  - When you browse, do you know “who” keeps track of “what” and do you “care”? “Who” might be the browser software, the operating system, the computer owner, an eavesdropper on the network, the web site you are connecting to, etc.
  - To be specific, do you know what Amazon stores about your visits?
  - Have you ever read a site’s privacy policy?
- Cameras:
  - With tiny cameras and huge satellites, is there anything that you can expect not to be photographed?
  - Is there a technical “solution” (and what is the “problem”)?
- Location:
  - If your phone is on and in your pocket, who knows where you are?
  - If your car has “OnStar”, who knows where it is?
- Databases:
  - Who stores information about you and how carefully do they protect it?
  - Do you have a credit card, a grocery card, health insurance, voter registration, a loan, a Snapfish account, a Facebook account?
  - “Total Information Awareness”
- RFID (where to begin)

**Dangers:** What are the negative effects of privacy violations? Which matter to you?

- Economics: stolen credit cards, corporate espionage, ...
- Embarrassment: personal photos, health records, ...
- Safety: lock-cracking, blackmail, ...
- Totalitarianism: squashing dissent, “guilt by association”

**Analogies:** Before computers, there were privacy issues, which of course differed by culture, country, etc. Which provide guidance for digital privacy issues? Examples:

- Should it be private what books you borrow from a public library?
- When should the government be allowed to tap a phone line?
- Should cryptography be regulated to prevent “too much privacy”?
- Should the developer of photos showing a crime (have to) report the photos?

**Personal preferences:** What privacy would you give up to get something of value in return?

- 1GB of email storage if scripts run over your email?
- Grocery discounts in return for tracked buying habits?
- Money to be on a “reality television” show?

**Societal ethics questions:**

- Should a government be able to spy on its citizens? What about noncitizens?
- What safeguards should an entity have to have when storing “personal data”?
- Should privacy laws be tied to the technology (e.g., phone lines vs. email) or the activity (e.g., two-person personal communication)?
- If information is public, is it “more ethical” to make it more difficult to get? (For example, if you can get divorce records from the County office, why not put them on the Web?)
- Is privacy something only the “bad guys” want? What if the spies are the “bad guys”?
- If technology can be used for “good or evil” (e.g., satellite imaging), then are the technology developers simply “amoral” with no need to concern themselves with applications?
- Was privacy a “historical anomaly” between the epochs of small clans and the single global community?

**Stranger than fiction:**

- An MIT graduate student learned a governor’s health records by combining a freely available database of health-insurance claims with public voter-registration information.
- Until very recently, some standard cryptography protocols were deemed “munitions” by the U.S. government, making it illegal to “export” them, so web browser downloads had to check where you lived.
- Under http 1.0, it is easy to determine what (static) site someone is visiting based only on the size of the site and the size of the embedded images, even if the name of the site and all the content is encrypted.
- The state of Washington owns your instructor’s office phone and computer. The state can access the phone log (numbers dialed and length of calls), but cannot record the calls. The state can access the contents of email.