Privacy

- **Taxonomy of Privacy**
  - Understanding Privacy, Daniel Solove, MIT Press 2008

- **Information Processing**
  - Aggregation
  - Identification
  - Insecurity
  - Secondary Use
  - Exclusion

---

Solove’s Taxonomy

- **Aggregation**
  - Government
  - Consumer business
  - Credit business

- **Data mining yields “unsettling facts”**

- **Digital dossier**
  - Is it you?

- **Sex offender laws**
- **Bad data issues**

---

Taxonomy continued

- **Insecurity**
  - Identity theft
  - Distortion (false facts)

- **Govt, Industry must maintain privacy**
  - Data storage
  - Data access

- **Secondary Use**
  - Using data for purpose other than original intent
  - Fingerprints for govt employees

- **Who owns information?**
  - Company
  - Individual

---

Taxonomy Finished

- **Exclusion**
  - How is data modified and fixed?
  - Access to credit report

- **People should be told about data**
- **How is data shared**

- **Info. Dissemination**
  - Kiss and tell
  - Medical
  - Breach of trust

- **Notification on release of record?**
  - Expectation
From Privacy to Cryptography

- How do we keep digital information private?
  - Keep it to ourselves
  - Don’t go online
  - Use cryptography to protect it

- When should we really insist on security?
  - Facebook?
  - Bank?
  - Other?

Cryptography

- For encryption to work
  - Not to hard to encrypt (time, money)
  - Easy to decrypt if allowed (time, money)
  - Impossible to decrypt if not allowed (?)

- Mathematics is the basis for cryptography
  - Very hard to factor numbers
  - Very easy to determine if a number is prime
  - No “security through obscurity” publish methods

PKI: Public Key Infrastructure

- From PGP to Hushmail
  - PGP is “pretty good privacy”, Phil Zimmerman
  - Originally distributed in book form because of “munitions export restrictions” (1990’s, 40 bit)
  - Web of trust for public key/private key

- How do circumvent these systems?
  - Keylogging software by federal agents

Cryptography for the masses

- http://www.youtube.com/watch?v=ZDnShu5V99s
- http://www.youtube.com/watch?v=XeaZGt8_j1k
- http://www.catonmat.net/blog/musical-geek-friday-crypto/