
Chapter 4: What Did You Do Today?

- Record-keeping is easy: “data shadow”
- Personally stored email records
 - Note: hard to delete server-based email
 - Businesses often learn it’s a bad idea to keep this
- Records generated by routine actions — note inferences based on, i.e., time and location
- Are records accurate?

Building the Datasphere

- Create information worth collecting
- Make the data machine-readable (i.e., mag stripes, bar codes), OCR, RFID. (Note: separate readings on RFID later)
- Build a large database
Note: beware of secondary uses — *the* major privacy risk of such databases
- The Internet as a whole is a huge database
- Note the role of voluntary personal disclosures.
- Query: who has been surprised by someone's ability to dig up ancient personal disclosures. I have been. . .

Who Controls the Data?

- The subject?
- The aggregator?
- When people get worried enough about databases, they object and/or take countermeasures (i.e., bugmenot.com).

Chapter 6: Medical Records

- Note: significant changes as a result of the *Health Insurance Portability and Accountability Act* of 1996 (HIPAA); see <http://www.hhs.gov/ocr/hipaa/privacy.html>
- Note data shadow from insurance companies, pharmacists, etc.
- Legal issues sometimes overrule medical record privacy

Medical Insurance

- Patients must waive certain rights when dealing with health insurance companies
- Note the lack of accountability — insurance companies are generally not paid by the patient
- Secondary uses of data: hiring decisions

Medical Information Bureau

- Insurance company clearing house
- Prevent insurance fraud via omitted information
- Are they accountable? How do their practices match the Fair Information Principles?
- How does this affect patient care?

Computerized Records

- Slow movement
- Current issue: `http://www.nytimes.com/2005/02/19/business/19health.html`
- Easier to leak

Threats

- Innocent errors
- Abuse by insiders
- For-profit abuse by insiders
- Physical intruder
- Determined, malicious attackers

Conflicting Rights

- Insurance fraud vs. patient privacy
- Adopted children vs. maternal (and sometimes paternal) privacy
- Computerized records' efficiency vs. privacy

Chapter 7: Marketing

- Secondary uses — address-change database
- Automobile registrations plus census tract: combining databases
- Transaction-level info
- Who owns the information?
- Online data collection from children restricted by law: <http://www.cdt.org/legislation/105th/privacy/coppa.html>
- Opt-out vs. opt-in
- International aspects of enforcement