Cyberculture and Privacy

(Notes based on Sara Baase, “A Gift of Fire” Chp 2)
Cyberculture and Privacy

A. Computers and Privacy

*Computers are not needed for the invasion of privacy.*

1. **Computers** do make new threats possible and old threats more potent, however.

2. **Privacy** can mean:
   - *Freedom from intrusion* into personal life.
   - *Control of information* about oneself.
   - *Freedom from surveillance*.
Cyberculture and Privacy

B. Style

1. Primary Use
   • Example: IRS data used to establish tax owed;

2. Secondary Use
   Using information for a purpose other than the one for which it was obtained. Some examples:
   • Sale (or trade) of consumer information to other businesses.
   • Credit check by a prospective employer.
   • Government agency use of consumer database.
Cyberculture and Privacy

C. Method:

1. Oblique Information Gathering:
   - You are asked and willingly provide primary-use information;

2. Transparent Information Gathering:
   - Satellite surveillance
   - Caller ID
   - Supermarket cards
   - Web-tracking data; cookies.
   - Peer-to-peer monitoring (remote desktop/ WMA licenses)
   - 800- or 900- number calls (or the pizza place)
   - How could this (pizza place example) happen? Smart Cards (programming – in the news – pro – con), e.g., or using the Internet (it is an effect of the blending of public and private sociocultural space)
Cyberculture and Privacy

C. Method:

3. Data Mining

Accumulating massive amounts of information. Some examples:

• Sharing of business or government databases to detect fraud by recipients of government programs, or to analyze criminal background for elections.

• Ex: Choicepoint

Choicepoint and the 2000 election
Citibank (see handout)
Cyberculture and Privacy

D. Uses:

1. Computer Matching

Combining and comparing information from more than one database. Some examples:

• Sharing of government agencies’ databases to detect fraud by recipients of government programs.
• Creating consumer dossiers from various business databases.
• Sharing cross-state law enforcement info
2. Personal Profiling

Using data in computer files to predict likely behaviors of people. Some examples:

- Businesses engage in profiling to determine consumer propensity toward a product or service.
- Government agencies use profiling to create descriptions of possible terrorists.
Cyberculture and Privacy

D. Uses

3. Monitoring and Tracking

Examples:
- GPS (global positioning system).
- Cell-phones.
- Black boxes in automobiles.
- Other wireless appliances.
E. Big Brother

i. Federal Government Databases

Purpose:
- Determine eligibility for jobs and programs.
- Reduce waste.
- Detect fraud.
- Law enforcement: CARNIVORE (DCS1000); CALEA; Linkswarm article

Regulations:
- Privacy Act of 1974.
E. Big Brother

ii. 4th Amendment

a. Expectation of Privacy:
   - Government’s rights are limited.
   - Government must have probable cause to search private premises or seize documents.

b. Privacy Challenges:
   - New sensing and surveillance technologies enable the government access to private premises without physical entry.
   - New technologies provide the government with access to huge amounts of personal data in business databases.
   - Courts allow some searches and seizures of computers without search warrants.

c. Foreign Government Law
   ex: China and Google
E. Big Brother

iii. National ID Card System (driver’s license, smart cards, e.g.)

If implemented today, the card would contain your:

- Name.
- Address.
- Telephone number(s).
- Photo.
- SSN.

The system could potentially allow access to your:

- Medical information.
- Tax records.
- Citizenship.
- Credit history.
- Much more...
F. Privacy Enhancing Technologies

- Cookie/Adware disablers
- Opt-in/opt-out options
- Anonymous Web services
- PGP, Encryption, P3P
- ‘Good’ passwords (what makes one good?)
- Audit trails (particularly important for e-voting)