1

CPSC 181
Computers and Society

Spring 2010
Prof. Jennifer Welch

2

Sources

- Sara Baase, *A Gift of Fire, Second Edition*, Pearson Education Inc., 2003
  - primary source
- Michael J. Quinn, *Ethics for the Information Age*, Pearson Education Inc., 2005
- J. Glenn Brookshear, *Computer Science An Overview*, Eighth Edition, Pearson Education Inc., 2005

3

Studying the Impact of Computers

- Using tools of historians and sociologists
- Using legal analyses
- Using ethical frameworks
  - focus of the Quinn book
  - cf. ENGR 482, Ethics and Engineering

4

Some of the Benefits of Computers

- entertainment
- communication (email, web)
- education and training
- crime fighting
- health and medicine
- tools for disabled people
- industrial automation
- reducing paper use and trash
- what else?

5

Some Issues with the Use of Computers

- privacy and personal information
- encryption and interception of communications
- reliability and safety
- freedom of speech
- intellectual property
- computer crime
- computers and work
- professional ethics
- what else?

6

Privacy

- three aspects of privacy
  - freedom from intrusion (being left alone)
  - control of information about yourself
  - freedom from surveillance (being followed, watched, eavesdropped on)
- is privacy a good thing?
  - some criticisms: allows deception, hypocrisy, wrongdoing, fraud,…
  - but let's assume it mostly is
- tradeoff privacy for other benefits to self and society
- computer technology "has made new threats possible and old threats more potent" (Baase)

7

Factors to be Balanced Against Privacy

- protect personal and group privacy against unjustified intrusions
- collect information needed for sensible decision-making in society, business, and government
- protect public order and safety with constitutionally limited government surveillance

8

How Technology Puts Privacy at Risk

- gathering information about you without your knowledge and consent
  - supermarket discount cards
  - ISPs (keep track of what web sites you visit)
  - cookies (a web site stores information on your computer)
    - DoubleClick, a web advertising company, got people's financial information from a Quicken website

9

What Happens to Your Information?

- Since it is so easy to copy, distribute, and analyze data relating to computer use, there has been a surge in *secondary use* of the information:
  - in the old days, postings to Usenet newsgroups were thought to only be recorded for a few days. But there were some archives and now, for instance, employers can search these archives for postings made by potential employees
  - computer profiling by businesses (find prospective customers) and law enforcement (find prospective criminals)

10

Databases

- Federal government has thousands of databases about us
  - government jobs and benefits
  - detect fraud
  - collect taxes
  - catch criminals
- Need to balance legitimate interest vs. illegitimate uses

11

Federal Privacy Laws

- 1974: Privacy Act, in response to abuses in 1960's and early 1970's
  - tracking people not wanted for any crime but just because of their political views (e.g., opposed the Vietnam war, were civil rights activitists)
  - Privacy Act requires written consent of subject before disclosing information (with 12 exceptions)
- 1988: Computer Matching and Privacy Protection Act
  - requires gov't agencies to follow a review process before doing *computer matching* (combining and comparing info from different databases)

12

Federal Privacy Laws Not Strong

- 1974 law has "many loopholes, weak enforcement, and only sporadic oversight"
- Congressional investigation regarding 1988 law found that agencies were very careless about following it
  - Selective Service bought birthday list from an ice cream company to find young men who had not registered for the draft
  - Would you like the IRS to calculate your income based on a boast you put into an on-line dating service?

13

Ways Around Laws

- Many government agencies (IRS, FBI, INS, etc.) collect personal data from private companies
  - this way they get information that might be illegal or controversial for them to collect
- ChoicePoint is a private company that gathers data from credit bureaus, telephone records, liens, deeds, drug tests, doctors' backgrounds, insurance fraud, other gov't agencies
  - has contracts with the Justice Department and IRS, and has a web site for FBI agents
  - was fined $1.37 million by state of Pennsylvania for selling driver data - breach of contract with the state

14

Burden of Proof vs. Fishing Expeditions

- Do databases and search technologies just make law-enforcement more efficient?
- Or do they fundamentally undermine the notion of ”presumed innocent until proven guilty"?

15

Violations of Privacy Laws by Government Agencies

- Several investigations by the Government Accountability Office (GAO), Congress' "watchdog" agency
- in 1997, 80% of gov't websites linked from the White House webpage violated the Privacy Act
- Many agencies' websites still use cookies, which probably violate the Privacy Act

16

Violations of Privacy Laws by Government Agencies and/or Employees

- FBI's National Crime Information Center (NCIC) database has been misused by employees of law-enforcement agencies by
  - selling info to private investigators
  - snooping on political opponents
  - altering or deleting information
  - stalking and murdering
- Many such stories about the IRS

17

The Fourth Amendment

- "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
- Problem is that much of our personal information is in huge databases outside of our control.

18

Infringements on 4th Amendment

- FBI can get some information from your credit report without a court order
- FBI can get your student records without a court order
- Law enforcement agencies can get your medical records without a court order
- Thanks to the Patriot Act, the gov't can get info from financial institutions on any transactions that "differ from [your] usual pattern" without a court order
- What info should the gov't be able to get about your web search activities without a court order?

19

Does Any of This Bother You?

- Remember when Japanese-Americans (U.S. citizens) were rounded up into concentration camps during World War II, just for being of Japanese descent?
- The government got the information about them from the Census Bureau.

20

More Ways that Technology Erodes 4th Amendment Protection

- Satellite surveillance
  - used to find people growing marijuana, growing cotton without a permit, or building without a permit
  - is this searching without a court order? Supreme Court has not ruled directly on this
  - In 2001, Supreme Court ruled police cannot use thermal imaging devices to search a home from the outside without a search warrant
- Automated toll collection
- Itemized purchase records

21

More Search and Surveillance Tools

- Electronic body searches
  - machine scan is less intrusive than a "pat down" search
  - but shows your body in detail, and the image can then be stored and copied
- Does your comfort level with the use of this device depend on who it is used on?
  - everyone, or just "suspicious" people? Use of this machine at Kennedy airport in 2000 found 5% of suspected drug smugglers actually carrying drugs

22

Video Surveillance & Face Recognition

- Video cameras have long been used for security in banks, prisons, etc.
- When used with face recognition systems, stakes are raised.
  - drivers license photos from several states were bought by a private company in 1999 and put in a database
  - Police scanned faces of everyone who attend the 2001 Super Bowl, then searched computer files of criminals for matches; later used in local restaurants and clubs

23

Video Surveillance & Face Recognition

- Issues:
  - like a police lineup, without your knowledge or consent
  - face-recognition systems are not very accurate
  - is potential benefit (e.g., tracking criminals, including young people violating a curfew) worth possible misuse (tracking political dissidents, journalists, political opponents of powerful people)?
  - Should it be used only in certain situations and for certain classes of illegal behavior?
  - Should people be informed when cameras are in use?

24

Consumer Information

- Businesses use software to analyze consumer data and government records to find potential new customers
- Example of *data mining*: searching large amounts of data to find new information
- Positive aspects:
  - get material, coupons, and recommendations tailored to your own interests
- Negative aspects?

25

Credit Bureaus

- Central storehouse of information for evaluating applications for credit
- Sometimes used by employers for background checks
- Federal law before 1996 allowed easy access to your credit report for other purposes (e.g., embarrass political rival)
- Law in 1996 limited old negative information (e.g., bankruptcies, criminal convictions)
  - is this good (privacy protection) or bad (restricting flow of relevant information)?

26

Credit Bureaus

- Used to sell mailing lists to marketers
  - had catalogs describing and promoting different kinds of lists available (e.g., "highly affluent, "people in financial difficulties")
  - They eventually stopped this due to public pressure and lawsuits
- They also used to sell "header" information (name, address, phone, SSN) from credit files
  - 2001 ruling made this illegal without consumer consent

27

Privacy Principles for Personal Data

- collect only needed data
- inform people about the data collection and how the data will be used
- offer a way for people to opt out
- use opt-in policy for sensitive data (like medical)
- keep data only as long as needed
- maintain accuracy and security of data
- provide way for people to access and correct the data about themselves

28

National ID Card?

- Social security numbers are highly insecure
  - appear on numerous public documents
- yet they are used as identifiers in many databases
  - bank accounts, IRS,…
- Other flaws:
  - they are *not unique* (about 10 million duplicate numbers)
  - easy to forge, numbers rarely verified
- Should we institute a new, more secure, numbering system?

29

National ID Card?

- Proposed national ID card would be a "smart card" with name, photo, SSN, health, tax, financial, citizenship, fingerprints, retina scan,…
- Possible benefits:
  - harder to forge
  - authentication would reduce fraud
  - verify work eligibility
  - easier to track and identify criminals
- With a large and mobile population, having the government approve the hiring of every employee ever is only possible with computer support

30

National ID Card?

- Possible negatives:
  - threat to freedom and privacy (reminiscent of Nazi Germany or apartheid South Africa)
  - potential for abuse with regard to the information stored on the card
  - would this system reduce terrorist attacks? (several 9/11 hijackers had valid ID)
  - what happens if some part of the system is unreliable?
  - opportunities for overzealous surveillance
  - if someone did manage to steal your identity, s/he would have it *all*

31

Medical Information

- Medical records are becoming increasingly computerized
- Potential benefits:
  - improve medical care
  - lower costs
  - help protect privacy (from lab technicians, billing clerks, etc. who may not need to know the medical details but can anyway with paper records)
- Potential pitfalls:
  - privacy risks on a big scale: there can be serious negative consequences to someone if information is leaked concerning, say, psychiatric treatment, alcoholism, or sexually transmitted diseases

32

Medical Information

- Marketers love medical information
  - Metromail, a mailing-list broker, sold lists of people with specific diseases to the pharmaceutical industry
- We don't have much control over our medical records:
  - most people's medical bills are paid by third party insurance companies, which need access to the medical records

33

Some Privacy Enhancing Technologies

- disable or reject cookies with your web browser
- anonymizer.com provides a service for surfing the web anonymously - leave no record of sites visited
- Zero-Knowledge Systems, Inc. is developing "digital cash", so you can make purchases online that are not linked to your name with a credit card
- well-designed database for sensitive information includes features to prevent leaks, intruders, and unauthorized access (e.g., billing clerk can't see results of tests)

34

Thought Question

- A business gives free PCs and Internet services in exchange for tracking web activities.
  - fair option for consumers or
  - taking advantage of low-income people, who give up some privacy?

35

Thought Question

- A company plans to market a device you can wear that will make photos of you come out streaked and useless. It is marketed to celebrities (to foil the paparazzi).
  - Is this a triumph for personal privacy or
  - a deterrent to good law enforcement? (Remember security surveillance cameras)

36

Computers and Work

- Eliminate some jobs, create others
- Is it an overall win or lose?
- Probably overall a win, looking at 20th century and technology in general:
  - population of US quadrupled
  - yet unemployment rate in May 2004 was only 4%, less than most of the century
  - children *are* working less, though

37

Computers and Work

- Working environment has been affected
- More people can work at home than since the beginning of the Industrial Revolution
- Telecommuting benefits:
  - reduced overhead, increased productivity for employers
  - reduces traffic congestion, pollution, and energy use
  - provides options for elderly and disabled
  - provides flexible hours for parents
  - more flexibility to employees for where they live

38

Problems with Telework

- corporate loyalty is weaker
- some employees less productive, others work too much
- blurred boundary between work and home can be stressful
- social isolation, low morale

39

Changing Business Structures

- trend toward smaller businesses, more independent consultants and contractors
- flattening of hierarchies in large companies
- more empowerment of workers

40

Monitoring Employees

- Computers provide new ways to monitor employees, can be done constantly now with the results stored and searchable
- Monitor performance (keystrokes, customer-service calls, retail-clerk operations)
  - "electronic sweatshop"
- Monitor location (truck drivers, badges)
  - do you want your supervisor to know when you go to the bathroom?

41

Monitoring Employees

- Reasons to monitor email, voice mail, computer files:
  - find needed business info when employee is not available
  - protect security of proprietary info
  - prevent/investigate possible criminal activity (e.g., embezzlement)
  - prevent personal use of employer facilities
  - check for violations of company policy
  - investigate complaints of harassment
  - check for illegal software

42

Email Monitoring Example

- Most major stock brokerage companies use email filters to check for
  - illegal messages (exaggerating the prospects of some investment)
  - unethical messages (pressuring clients to buy or sell)
  - offensive email
- Use artificial intelligence techniques
- Does routine filtering violate the privacy of the brokers? If so, is it justified by the tradeoffs?

Web Surfing Monitoring

- Many major companies use software that analyzes the logs recording what websites their employees visit
- Some of them have filtering software
- Is non-work web surfing a serious problem or is it like reading a newspaper at your desk?
- Note: Judges didn't like a policy that would have their own web/email use monitored -- are they willing to require other employers have the same trust in their employees?