Computers and Society

Privacy and the Laws Governing It

Notice: This set of slides is based on the notes by Professor Guattery of Bucknell and by the textbook author Michael Quinn

Some Stories

• In the US in 1989 an actress opened her door and was shot dead by a stalker. The stalker had gotten her address through the motor vehicles department (such information is no longer sold).

• It was recently revealed that iPhone and Android apps were downloading users' address books without telling them. Other apps on these devices were downloading photographs without notice.

More Stories

• In Britain, a tabloid newspaper secretly accessed the voice mail of a missing girl without permission. This access falsely gave the girl's family hope that she was still alive.

•In Britain, many public areas are watched by hundreds of surveillance cameras.

• There are numerous examples where the lives of celebrities or politicians have been invaded by the press.

Privacy

All of these examples illustrate *privacy* issues. What do you think about the situations? Are you concerned or unconcerned about them?

What is privacy, and what privacy rights should an individual have?

Privacy Definition

18th century British philosopher Edmund Burke specified that there is a "zone of inaccessibility" surrounding a person. A person has *privacy* to the extent that he or she controls access to that zone.

Important question: How big should that zone be, and what control should an individual have over access to it?

Privacy Pros and Cons

Positive aspects of privacy: Privacy allows one to express oneself freely outside the public sphere. It provides protection from harassment by the government and by other individuals.

Negative aspects of privacy: Privacy can be used to cover crimes and antisocial behavior.

Threats to Privacy

Daniel Solove (2006)

• **Information collection**: individuals and organizations can gather information that can be used for other purposes
• **Information processing**: activities such as data mining can be used to draw conclusions about collected data.
• **Information dissemination**: collected data can be distributed to harass or embarrass one
• **Invasion**: individuals or organizations can interfere in one's life

https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf

Types of Information

• **Public Information**: information provided to an organization with a right to share (for example, directory information); may be limited

• **Personal Information**: information an individual does not want to share (account numbers, facts such as religious affiliation)

• **Public Records**: birth/death certificates, marriage licenses, criminal records, motor vehicle records; not always public information

Examples of Privacy Concerns

Here is a list of some privacy concerns that people have expressed. What do you think about these issues?

• customer loyalty programs
• security scanners
• automobile "black boxes"
• web browser cookies
• RFID cards and similar technology
• computer spyware
• social networks (e.g., data shared with apps)
• DVRs

What is the Role of Government?

The US has many laws governing privacy. There are many that protect privacy, but some may go too far. For example, HIPAA (Health Insurance Portability and Accountability Act) included provisions to insure that an individual's medical information would be kept private. As a result it became difficult, for example, for spouses to get information, or for parents to get information about children over 18.

Role of Government? (2)

On the other hand, the US government has passed many laws to limit privacy. These are usually created to increase security:

• Security screening
• PATRIOT (Providing Appropriate Tools Required to Intercept and Obstruct Terrorists) Act
• Crime information databases.

A Balancing Act

- Federal, state, and local governments in United States have had significant impact of privacy of individuals
- Government must balance competing desires
  - desire to be left alone
  - desire for safety and security
- National security concerns increased significantly after 9/11 attacks

U.S. Legislation Restricting Information Collection

Employee Polygraph Protection Act

- Passed in 1988
- Prohibits private employers from using lie detector tests under most conditions
- Cannot require test for employment
- Exceptions
  - Pharmaceutical companies and security firms may give test to certain classes of employees
  - Employers who have suffered a theft may administer tests to reasonable suspects
  - Federal, state, and local governments exempt

Children's Online Privacy Protection Act

- Reduces amount of public information gathered from children
- Online services must gain parental consent before collecting information from children 12 and under

Genetic Information Nondiscrimination Act

- Health insurance companies
  - Can't request genetic information
  - Can't use genetic information when making decisions about coverage, rates, etc.
  - Doesn't apply to life insurance, disability insurance, long-term care insurance
- Employers
  - Can't take genetic information into account when hiring, firing, promoting, etc.
  - Small companies (< 15 employees) are exempt

Information Collection by the Government

Census Records

- Census required to ensure every state has fair representation
- Number of questions steadily rising
- Sometimes Census Bureau has broken confidentiality requirement
  - World War I: draft resistors
  - World War II: Japanese-Americans

Internal Revenue Service Records

- The 16th Amendment to the U.S. Constitution gives the federal government the power to collect an income tax
- IRS collects more than $2 trillion a year in income taxes
- Income tax forms contain a tremendous amount of personal information: income, assets, to whom you make charitable contributions, medical expenses, and more

FBI *N*ational *C*rime *I*nformation *C*enter

- NCIC (established 1967, current version 2000)
  - Collection of databases related to various crimes
  - Contains > 39 million records
- Successes
  - Helps police solve hundreds of thousands of cases every year
  - Helped FBI tie James Earl Ray to assassination of Dr. Martin Luther King, Jr.
  - Helped FBI apprehend Timothy McVeigh for bombing of federal building in Oklahoma City

OneDOJ Database

- Database being constructed by U.S. Department of Justice
- Gives state and local police officers access to information provided by five federal law enforcement agencies
  - Incident reports
  - Interrogation summaries
  - Other information not available through NCIC
- Criticisms
  - OneDOJ gives local police access to information about people who have not been charged with a crime
  - There is no way to correct misinformation in raw police reports

Closed-circuit Television Cameras

- First use in Olean, New York in 1968
- Now more than 30 million cameras in U.S.
- New York City's effort in lower Manhattan
  - $201 million for 3,000 new cameras
  - License plate readers
  - Radiation detectors
- Effectiveness of cameras debated

Covert Government Surveillance

4th Amendment to U.S. Constitution

"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."

Wiretaps and Bugs

- *Omstead v. United States* — wiretapping OK
- Federal Communications Act — wiretapping made illegal
- *Nardone v. United States* — wiretapping not OK
- FBI continues secret wiretapping
- *Katz v. United States* — bugs not OK

Carnivore Surveillance System

- Created by FBI in late 1990s
- Monitored Internet traffic, including email exchanges
- Carnivore = Windows PC + "packet-sniffing" software
- Captured packets going to/from a particular IP address
- Used about 25 times between 1998 and 2000
- Replaced with commercial software

Covert Activities after 9/11

- September 11, 2001 attacks on World Trade Center and Pentagon
- President Bush authorized new, secret, intelligence-gathering operations inside United States

National Security Administration Wiretapping

- President Bush signed presidential order
  - OK for NSA to intercept international phone calls & emails initiated by people inside U.S.
  - No search warrant required
- Number of people monitored
  - About 500 people inside U.S.
  - Another 5,000-7,000 people outside U.S.
- Two al-Qaeda plots foiled
  - Plot to take down Brooklyn bridge
  - Plot to bomb British pubs and train stations
- Snowden leak since June 2013

TALON Database

- Created by U.S. Department of Defense in 2003
- Supposed to contain reports of suspicious activities or terrorist threats near military bases
- Reports submitted by military personnel or civilians
- Reports assessed as "credible" or "not credible" by military experts
- Reports about anti-war protests added to database
- Many of these reports later deleted from database
- In 2007 new Under Secretary of Defense for Intelligence recommended that TALON be terminated

U.S. Legislation Authorizing Wiretapping

Title III

- Part of Omnibus Crime Control and Safe Streets Act of 1968
- Allows a police agency with a court order to tap a phone for up to 30 days
- In 1972 U.S. Supreme Court again rejected warrantless wiretapping, even for national security

Electronic Communications Privacy Act

- Passed by Congress in 1986
- Allows police to attach two kinds of surveillance devices to a suspect's phone line
  - Pen register: displays number being dialed
  - Trap-and-trace device: displays caller's phone number
- Court order needed, but prosecutors do not need to show probable cause
- Allows police to do roving wiretaps (following suspect from phone to phone)

Stored Communications Act

- Part of Electronic Communications Privacy Act
- Government does not need a search warrant to obtain from an Internet service provider email messages more than 180 days old
- Advent of cloud computing raises new privacy concerns
- Digital Due Process organization (nearly 50 companies and privacy rights organizations) lobbying Congress to change law

Communications Assistance for Law Enforcement Act

- Passed in 1994
- Designed to ensure police can still do wiretapping as digital networks are introduced
- FBI asked for new abilities, such as ability to intercept digits typed by caller after phone call placed
- Federal Communications Commission included these capabilities in its guidelines to phone companies
- Privacy-rights advocates argued that new capabilities went beyond Congress's intent