Privacy

CSE 312 – Legal, Social, and Ethical Issues in Information Systems

Stony Brook University

http://www.cs.stonybrook.edu/~cse312

Ch 2: Privacy

2.1 Privacy Risks and Principles

2.2 The Fourth Amendment, Expectation of Privacy, and Surveillance Technologies

2.3 The Business and Social Sectors

2.4 Government Systems

2.5 Protecting Privacy: Technology, Markets, Rights, and Laws

2.6 Communications

2.1 Privacy Risks and Principles

- What is privacy?
  - Freedom from intrusion (being left alone)
  - Control of information about oneself
  - Freedom from surveillance (from being tracked, followed, watched)
- Invasion of privacy:
  - East Germany Stasi (the secret police) files:
    - The informers were neighbors, co-workers, friends
  - Private investigators search household garbage for medical and financial information, details of purchases, evidence of romantic affairs

Privacy Risks and Principles

- Privacy is a good thing
- Critics of privacy argue that it gives cover to wrongdoing.
  - "What do you have to hide?"
- The desire to keep things private does not mean we are doing anything wrong:
  - We might wish to keep health, religion, political views, relationship, and family issues private!
  - Privacy can be important to safety and security.
  - Kinds of private information: home address and phone number, SSN, financial data, travel plans, etc.

Privacy Risks and Principles

- Privacy threats:
  - Intentional, institutional uses of personal information (in the private sector primarily for marketing and decision making)
  - Unauthorized use or release by "insiders" (the people that have access to the information)
  - Theft of information
  - Inadvertent leakage of information through negligence or carelessness
  - Our own release when we are not aware of the risks

Privacy Risks and Principles

- What is in your mind is private!
- But we cannot expect complete privacy
  - what people know from conversations and observing is not private: acquaintances know what you look like, where you work, what kind of car you drive, and whether you are a nice person.
    - They don't need permission to talk about you (covered by Freedom of Speech)
    - If you live in a small town, you have little privacy; everyone knows everything about you.
    - In a big city, you are more nearly anonymous.
  - We give up some privacy for the benefits of dealing with strangers:
    - We give a lot of information when we rent a place to live, get hired, buy automobile insurance, apply for a credit card, bank account, mortgage

Privacy Risks and Principles

New Technology, New Risks

- We are more connected than ever before in history, but we are less private than even before

Privacy Risks and Principles

New Technology, New Risks

- Computers and the Internet with their increases in storage space and connectivity, make collection and searching for date much cheaper and easier
  - but when this information is about us, the same capabilities threaten our privacy
- Databases contain private information about us:
  - IRS has our taxes
  - Our doctors have our health information
  - Our school has our grades

Privacy Risks and Principles

New Technology, New Risks:

Search query data

- Search engines collect many terabytes of data daily
- Searches are full of private information (SSN number, names)
- Data is analyzed to target advertising and develop new services
- Who gets to see this data?
- In 2006, the federal government presented Google with a subpoena for two months of user search queries and all the Web addresses that Google indexes.
  - A court reduced the scope of the subpoena removing user queries

Privacy Risks and Principles

New Technology, New Risks:

Search query data

- In 2006, AOL put online months of search data for research
  - 20 million search queries by more than 650,000 people from a three-month period
  - The data identified people by coded ID numbers, not by name
  - It was not difficult to deduce the identity of some people, especially those who searched on their own name or address
  - Some searches were bizarre or illegal
  - led to the resignation of AOL's CTO and two employees were fired: the researcher who released the data and his immediate supervisor
  - removed the data in a few days, but it is still available

Privacy Risks and Principles

New Technology, New Risks:

Smartphones

- Location apps
  - not only GPS
  - but also the location of nearby cell towers
- Data sometimes stored and sent without user's knowledge
  - half the apps in one test sent the phone's ID number or location to other companies (in addition to the one that provided the app)
  - other data is sent (gender, email)
- Some iPhones stored months of data, in a hidden file, about where the phone had been and when
  - Data in such files are vulnerable to loss, hacking, and misuse

Privacy Risks and Principles

- Advertisement for dial telephone service available to delegates to the 1912 Republican convention in Chicago.
- A major selling point of dial telephone service was that it was "secret", in that no operator was required to connect the call.

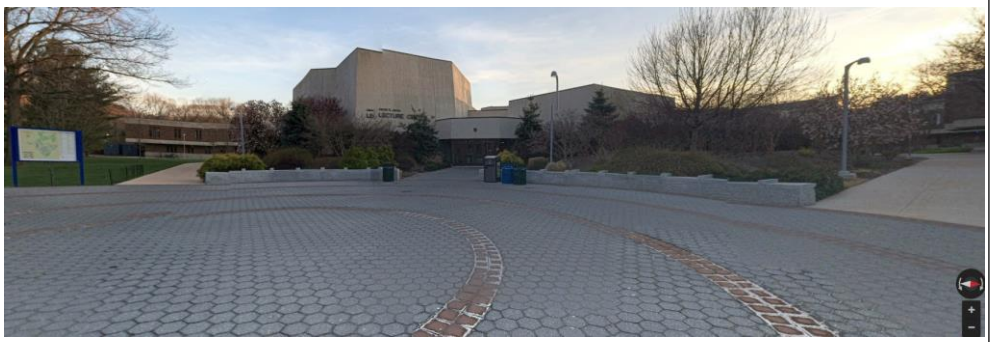
Privacy Risks and Principles

New Technology, New Risks:

Google's Street View

- Austria: Google Street View was banned in Austria because Google was found to collect Wifi data unauthorized in 2010.
- Blurs images of faces

Stony Brook Javits



Privacy Risks and Principles

New Technology, New Risks

Summary of Risks:

- Anything we do in cyberspace is recorded
- Huge amounts of data are stored
  - People are not aware of all the collection of data
- Software is complex and Leaks happen:
  - Files on hundreds of thousands of students, applicants, faculty, and/or alumni from the University of California, Harvard, Georgia Tech, Kent State, and several other universities, some with Social Security numbers and birth dates were stolen by hackers
  - Records of roughly 40 million customers of TJX discount clothing stores (T.J. Maxx, Marshalls), including credit and debit card numbers and some driver's license numbers were also stolen by hackers

Privacy Risks and Principles

New Technology, New Risks

Summary of Risks:

- If information is on a public Web site, it is available to everyone.
- Data collected for one purpose (such as, responding to a search query) will find other uses (such as, tracking, marketing, or criminal investigations).
- People depend on the businesses and organizations that manage their information to protect it from thieves, accidental collection, and leaks

Privacy Risks and Principles

New Technology, New Risks

- Information on the Internet lasts forever.
- Government can request sensitive personal data held by businesses or organizations.

Privacy Risks and Principles

Terminology

- *Personal information* – any information relating to an individual person.
  - It may also include: phone number, identification number, email, or even user name.
- *Informed consent* – users being aware of what information is collected and how it is used
  - A person can decide, according to his or her own values, whether or not to interact with a business or organization or whether to use the device or application

Privacy Risks and Principles

Terminology

- *Invisible information gathering* - collection of personal information about a user without the user's knowledge.
  - A car rental company recorded the driving speed and whether or not the driver is wearing a seatbelt
  - A company offered a free program that changed a Web browser's cursor into a cartoon character. Millions of people installed the program but then later discovered that the program sent to the company a report of the websites its users visited, along with a customer identification number in the software.

Privacy Risks and Principles

Terminology:

- *Cookies* – Files a Web site stores on a visitor's computer
  - contains the visitor's activity
  - a retail store may store what products were watched
  - On subsequent visits, the site retrieves information from the cookie
  - "supercookies" recreate deleted cookies and are difficult to find and remove

Privacy Risks and Principles

Terminology:

- *Secondary use* – Use of personal information for a purpose other than the purpose for which it was provided.
  - sale of consumer information to marketers
  - *Data mining* – Searching and analyzing masses of data to find patterns and develop new information or knowledge.
    - *Matching* means combining and comparing information from different databases
    - *Profiling* means analyzing data to determine characteristics of people most likely to engage in certain behavior

Privacy Risks and Principles

- After informing people about what personal information an organization collects and what it does with that information (*privacy policy*), give people some control over secondary uses
- Two common forms for providing informed consent are *opt out* and *opt in*:
  - *opt out* – Person must request (usually by checking a box) that an organization *not* use information.
  - *opt in* – The collector of the information may use information only if person explicitly permits use (usually by checking a box).
- Opt-out options are now commonly the default
  - Responsible, consumer-friendly companies often set the default so that they do not share personal information and do not send marketing emails unless the person explicitly allows it.

Privacy Risks and Principles

Discussion Questions

- *Have you seen opt-in and opt-out choices? Where?*
- *Did you read what you agreed to?*
- *How were they worded?*
- *Were any of them deceptive?*
  - *online opt-in choices may be pre-checked and require you un-checking the box to avoid opting in*
  - *"subject to change without notice" clause found in most privacy policies*

Privacy Risks and Principles

Fair information principles

1. Inform people when you collect information.
2. Collect only the data needed.
3. Offer a way for people to opt out.
4. Keep data only as long as needed.
5. Maintain accuracy of data.
6. Protect security of data.
7. Develop policies for responding to law enforcement requests for data.

- The United States Federal Trade Commission's Fair Information Practice Principles (FIPPs) are guidelines, recommendations for maintaining privacy-friendly, consumer-oriented data collection practices, and are not enforceable by law.

https://en.wikipedia.org/wiki/FTC_Fair_Information_Practice

- Law in European Union: Data Protection Directive 95/46/EC (adopted in 1995)

https://en.wikipedia.org/wiki/Data_Protection_Directive

Transparency, Legitimate purpose (Personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes), Proportionality (may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected)

2.2 The Fourth Amendment, Expectation of Privacy, and Surveillance Technologies

The right of the people to be secure in their person, 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.

—4th Amendment, U.S. Constitution (1789)

The Fourth Amendment, Expectation of Privacy, and Surveillance Technologies

- Sets limits on government's rights to search our homes and businesses and seize documents and other personal effects. Requires government provide probable cause.
- Two key problems arise from new technologies:
  - Much of our personal information is no longer safe in our homes; it resides in huge databases outside our control.
  - New technologies allow the government to search our homes without entering them and search our persons from a distance without our knowledge.

The Fourth Amendment, Expectation of Privacy, and Surveillance Technologies

- The USA PATRIOT Act (passed after the terrorist attacks in 2001) eased government access to many kinds of personal information, including financial records, without a court order.

New Technologies

- Make possible "noninvasive but deeply revealing" searches
  - imaging systems (airport xrays to detect illegal objects on people, thermal-imaging devices to find heat lamps for growing marijuana)
  - location trackers (FBI put a location tracker on a student's car in California)
- *What restrictions should we place on their use?*
- *When should we permit government agencies to use them without a search warrant?*

Supreme Court Decisions and Expectation of Privacy

- *Weeks v. United States* (1914)
  - The American judicial system, including the Supreme Court of the United States, largely followed the precepts of English common law
  - The process by which the evidence was obtained had little, if anything to do with the permissibility of its use in court.
    - Fremont Weeks was convicted of using the mails for the purpose of transporting lottery tickets
    - At the time of his arrest, police officers went to Weeks' house to search it without a warrant
  - The United States Supreme Court unanimously held that the warrantless seizure of items from a private residence constitutes a violation of the Fourth Amendment

Supreme Court Decisions and Expectation of Privacy

- *Olmstead v. United States* (1928)
  - Supreme Court allowed the use of wiretaps on telephone lines without a court order.
  - Interpreted the Fourth Amendment to apply only to physical intrusion and only to the search or seizure of material things, not conversations.
    - Several petitioners, including Roy Olmstead, challenged their convictions, arguing that the use of evidence of wiretapped private telephone conversations amounted to a violation of the Fourth and Fifth Amendments.
    - Fifth Amendment to the United States Constitution protects a person from being compelled to be a witness against themselves in a criminal case.
      - "Pleading the Fifth": a witness can decline to answer questions where the answers might incriminate him

Supreme Court Decisions and Expectation of Privacy

- *Olmstead v. United States* (1928)
  - Supreme Court allowed the use of wiretaps on telephone lines without a court order.
  - Interpreted the Fourth Amendment to apply only to physical intrusion and only to the search or seizure of material things, not conversations.
    - Several petitioners, including Roy Olmstead, challenged their convictions, arguing that the use of evidence of wiretapped private telephone conversations amounted to a violation of the Fourth and Fifth Amendments.
    - Fifth Amendment to the United States Constitution protects a person from being compelled to be a witness against themselves in a criminal case.
      - "Pleading the Fifth": a witness can decline to answer questions where the answers might incriminate him

Supreme Court Decisions and Expectation of Privacy

- *Olmstead v. United States* (1928)
  - Supreme Court allowed the use of wiretaps on telephone lines without a court order.
    - In a 5-4 decision, the Court held that neither the Fourth Amendment nor the Fifth Amendment rights of the defendant were violated.
  - This decision was later overturned by Katz v. United States in 1967.

Supreme Court Decisions and Expectation of Privacy

- *Katz v United States* (1967)
  - Supreme Court reversed its position and ruled that the Fourth Amendment *does* apply to conversations.
    - Charles Katz used a public pay phone booth to transmit illegal gambling wagers from Los Angeles to Miami and Boston.
    - Unbeknownst to Katz, the FBI was recording his conversations via an electronic eavesdropping device attached to the exterior of the phone booth.
  - Court said that the Fourth Amendment protects people, not places
    - To intrude in a place where reasonable person has a reasonable expectation of privacy requires a court order.

Supreme Court Decisions and Expectation of Privacy

- Expectation of privacy:
  - *United States v. Miller, 1976*
    - The Supreme Court ruled that that if we share information with businesses such as our bank, then we have no reasonable expectation of privacy for that information
    - This interpretation is odd because we do expect that financial information is private
      - The case was complicated because it involved the Second Amendment to the United States Constitution (1791) (the right of the people to keep and bear arms) and the defendant was expected to go in the witness protection program because he testified against his gang members
        - National Firearms Act of 1934 requires certain types of firearms to be registered with the Miscellaneous Tax Unit (later the Bureau of Alcohol, Tobacco, Firearms, and Explosives)

Supreme Court Decisions and Expectation of Privacy

- *Kyllo v United States* (2001)
  - The Supreme Court ruled that police could not use thermal-imaging devices to search a home from the outside without a search warrant
    - The United States Department of the Interior used a thermal imaging device outside of Danny Lee Kyllo's home to find heat radiating from marijuana growing indoor lights
    - The Supreme Court stated that where "government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search.'"
    - The Supreme Court ruled 5-4 that the search was unreasonable and therefore unconstitutional.

Supreme Court Decisions and Expectation of Privacy

- *United States v. Jones (2012)*
  - The Supreme Court ruled that installing a Global Positioning System (GPS) tracking device on a vehicle and using the device to monitor the vehicle's movements constitutes a search under the Fourth Amendment.
    - The FBI installed a GPS on the car of Antoine Jones in 2004
    - The police had one argument: the vehicle drove around in public view
  - *How should we interpret "plain view"?*

Search and Seizure of Computers and Phones

- Warrants must specify exactly what is searched on computers or phones
- Suppose law enforcement agents have a search warrant for a computer but find that the files are encrypted
  - The Fifth Amendment to the U.S. Constitution specifies that a person cannot be forced to testify against himself
  - However, courts sometimes allow the government to require a person to provide keys or combinations to a safe
    - Rulings in federal courts have been inconsistent about whether such a requirement can apply to encryption keys.

Search and Seizure of Computers and Phones

- For many people the phone is a traveling office
  - Police may search an arrested person (without a search warrant) and examine personal property on the person
  - *Is the information on a phone included?*
    - The Ohio Supreme Court ruled that searching an arrested person's phone without a search warrant is unconstitutional
    - The California Supreme Court ruled otherwise
    - It was not yet heard by the U.S. Supreme Court
    - A federal appeals court ruled that customs agents do not need reasonable suspicion of a crime to search laptops, phones, and other electronic devices.

Video Surveillance and Face Recognition

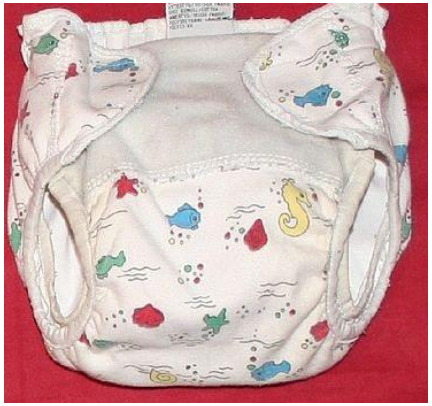
- Security cameras
  - Increased security
    - identified terrorists who set off bombs in the London subway and at Boston marathon
  - Decreased privacy
    - Many ordinary people do not like being tracked and photographed without their knowledge
  - Police in Tampa, Florida, scanned the faces of all 100,000 fans and employees who entered the 2001 Super Bowl (causing some reporters to dub it Snooper Bowl) to search for criminals.
    - People were not told that their faces were scanned
  - England was the first country to set up a large number of cameras in public places to deter crime
    - In 2005, the British government released a report saying Britain's closed-circuit TV systems were of little use in fighting crime
  - Clear limits for the technology and policy: events such as the Olympics

Video Surveillance and Face Recognition

- *Should we allow them to screen for people with unpaid parking tickets?*

2.3 The Business and Social Sectors Marketing and Personalization

- Marketing: finding new customers, members
  - Data mining: Online retailers make recommendations to you based on your prior purchases and on those of other people with similar buying patterns.
  - Targeted ads
    - Companies identifies young male adults who buy diapers and sends them coupons for beer because, with a new baby, they have less time to go to a pub



Marketing and Personalization

- Marketing
  - L.L. Bean, a big mail-order business, sends out fewer catalogs as it does a better job of targeting customers
  - The Democratic and Republican parties use extensive databases on tens of millions of people (job, hobbies, type of car, and union membership) to profile those who might vote for their candidates

Marketing and Personalization

- Informed consent
  - marketing is not unethical
  - Collection of consumer data for marketing without informing people or obtaining their consent was widespread, essentially standard practice, until roughly the late 1990s
  - Gradually, public awareness and pressure for improvement increased, and data collection and distribution policies improved.
  - Now we have federal regulations for informed consent
- "Do Not Track" button in browsers
  - The idea is that users would have one clear place to indicate that they do not want their Web activity tracked and stored.

Marketing and Personalization

- Paying for consumer information
  - Most companies give us free services for our information (e.g., GMail to mine our emails)
  - Some companies: when we fill out a contest entry form, we trade data for the opportunity to win prizes.
  - Lauren Weinstein, founder of Privacy Forum, argued that among less affluent people the attraction of free services may be especially strong, and it "coerces" them into giving up their privacy

Social Networks

- Two privacy concerns:
  - What *we* do
    - Post opinions, gossip, pictures, "away from home" status
    - Do people think about how the information might be used by others?
  - What *they* do
    - New services with unexpected privacy settings
      - Facebook News feeds and Photo tagging were introduced with the same visibility as wall pages
        - within a day people realized that it is easier to see the feed from everyone, then consulting their walls directly
        - tagging was introduced and people did not know how to turn off the feature that their friends can tag them in photos
        - According to the Federal Trade Commission (FTC), Facebook violated its stated policies in several instances

Life In the Clouds

- People often want a lot of information about others, but they do not want others to have access to the same kinds of information about themselves.
  - On Linkedin: people whose profiles we read know that we read them
- Convenience: we don't need to maintain our systems ourselves, we don't need to create backups, we can share documents
- The Web is public
  - Security of online data: consider if you put your information online
  - Millions of Americans do their taxes online and they are stored many years
  - Hospitals store their medical records online
  - *Is it safe?*

Location Tracking

- Global Positioning Systems (GPS) – computer or communication services that know exactly where a person is at a particular time
- Cell phones and other devices are used for location tracking
- Who might a person not want to get this information?
  - Thieves.
  - A stalker.
  - Co-workers or business associates.
  - A divorce lawyer.
  - An annoying or nosy neighbor.
  - Anyone else who might object to your religion, politics, or sexual behavior.

Location Tracking

- Tools for parents
  - GPS tracking via cell phones or RFID
  - Devices installed in a car tell parents where their teens are and how fast they are driving
  - Tracking children can increase safety
  - *At what age does tracking become an invasion of the child's privacy?*

A Right to Be Forgotten

- Right to Be Forgotten
  - People sometimes want to remove information about themselves from the Internet
    - Their photo on a friend's social network page or a photo-sharing site
    - A search query results with a person's name that a search engine returns
  - Practice in the European Union (EU, 1995) and Argentina since 2006
    - To exercise the right to be forgotten and request removal from a search engine, one must complete a form through the search engine's website
    - Google's removal request process requires the applicant to identify their country of residence, personal information, a list of the URLs to be removed along with a short description of each one, and attachment of legal identification.
  - In US it is a part of the policies of Web companies

2.4 Government Systems

Databases:

- Government Accountability Office (GAO) - monitors government's privacy policies
- Provisions of the Privacy Act of 1974:
  - Restricts the data in federal government records to what is "relevant and necessary" to the legal purpose for which the government collects it.
  - Requires federal agencies to publish a notice of their record systems in the Federal Register so that the public may learn about what databases exist.
  - Allows people to access their records and correct inaccurate information
  - Requires procedures to protect the security of the information in databases
  - Prohibits disclosure of information about a person without his or her consent (with several exceptions)

Government Systems

Databases:

- US Census: The U.S. Constitution authorizes and requires the government to count the people in the United States every 10 years, primarily for the purpose of determining the number of Congressional representatives each state will have.
  - Between 1870 and 1880, the U.S. population increased by 26%
    - It took 9 years to process the data
  - During the 1880s, the population increased by another 25%
    - Herman Hollerith, a Census Bureau employee, designed and built punch-card processing machines— tabulators, sorters, and keypunch machines— to process census data in 6 weeks
  - Census information is supposed to be confidential
    - During World War I, the Census Bureau provided names and addresses of young men to the government to help find and prosecute draft resisters

Government Systems

Databases:

- The U.S. Department of Education proposed establishing a database to contain the records of every student enrolled in a college or university in the United States.
  - The proposal would require colleges and universities to provide and regularly update the records including each student's name, gender, Social Security number, major, courses taken, courses passed, degrees, loans, and scholarships (public and private).
  - Pro: the federal government spends billions of dollars each year on federal grants and loans to students but has no good way to measure the success of these programs.

Public records: access vs. privacy

- Governments maintain "public records," that is, records that are available to the general public
  - Marriage license applications / Divorce proceedings

  - Property-ownership records

  - Bankruptcy records
  - Arrest records
  - Political campaign committees must report the name, address, employer, and donation amount for every donor who contributes more than $100 to a candidate for president
- These are public, but many are only available on paper in government offices
  - Lawyers, private investigators, journalists, real estate brokers, neighbors, and others use the records
- Privacy issue:
  - Public records include sensitive information such as Social Security numbers, birth dates, and home addresses
    - Maricopa County in Arizona, the first county to put numerous and complete public records on the Web, had the highest rate of identity theft in the United States

National ID Systems

- Social Security Numbers
  - SSNs first appeared in 1936 and were for the exclusive use of the Social Security program
  - In 1961, the IRS began using it as the taxpayer identification number
    - Employers require it
  - In 1976, motor vehicle departments received authority to use the SSN
    - Required it for new driving licenses

National ID Systems

- Social Security Numbers Problems
  - Too widely used
    - For many years the SSN was put on the insurance cards, student ID cards, faculty ID cards, many companies
  - Mistakes: A woman in Canada could not get her tax refund because the tax agency insisted she was dead.
    - Her identification number had been mistakenly reported in place of her mother's when her mother died.
    - The ID was described as a "license to exist."
  - Easy to falsify

National ID Systems

- Driving licenses
  - harder to forge
  - have to carry only one card
  - The REAL ID Act (2005) states that the driving license is accepted by the federal government for "official purposes" as defined by the Secretary of the United States Department of Homeland Security
    - Puts the burden on states to verify the data provided by the individuals (legal status in US)
      - Several states are not yet compliant with the law (2017)

National ID Systems

- Many European and Asian countries require national ID cards
  - The Indian government is building a national ID database for its 1.2 billion people.
    - The database will include each person's photo, fingerprints, iris scan, birth date.

- Opponents of national ID systems argue that they are profound threats to freedom and privacy
  - "Your papers, please" is a demand associated with police states and dictatorships.

2.5 Protecting Privacy: Technology, Markets, Rights and Law

Technology and Markets:

- Individuals, organizations, and businesses help meet the demand for privacy
  - They post free privacy-protecting software on the Web
  - Entrepreneurs build new companies to provide technology-based privacy protections
  - Businesses respond to consumer demand and improve policies and services
  - Activist organizations such as the Electronic Privacy Information Center inform the public, file lawsuits, and advocate for better privacy protection
  - Researchers invent new methods of encryption
    - Public-key cryptography

Protecting Privacy: Technology, Markets, Rights and Law

- Encryption is a technology, often implemented in software, that transforms data into a form that is meaningless to anyone who might intercept and view it
  - People are often not even aware that they are using encryption
    - The software handles it automatically
  - It is the best protection for data on laptops and other small data storage devices carried outside an office.
- Cryptographic software
  - Many Email clients (e.g., Apple Mail, Thunderbird)
  - Secure Messaging
  - Disk encryption
  - Anonymity networks

Protecting Privacy: Technology, Markets, Rights and Law

- Encryption generally includes a *coding scheme* or *cryptographic algorithm*, and specific sequences of characters called *keys*, used by the algorithm
- Applications:
  - Digital signature technology allows us to "sign" documents online
    - American Medical Association issues digital credentials to doctors that a laboratory website can verify when a doctor orders patient test
  - Digital cash and encryption-based privacy-protected transaction methods let us do secure financial transactions electronically without the seller acquiring a credit card or checking account number from the buyer

Encryption Policy

- Many cryptographers in the United States worked for the National Security Agency (NSA)
- Government ban on export of strong encryption software in the 1990s
  - The government interpreted anything posted on the Internet as effectively exported
    - That included researchers
  - Mostly removed in 2000

Encryption Policy

- *Audit trail*: the system keeps track of information about each access (ID of the user that accessed the data, read and write)
- Third-party *privacy audits* for companies: check for leaks of information, review the company's privacy policy and its compliance with that policy
  - large organizations have a position called *chief privacy officer* to check the privacy policy
- Several companies (IBM, Microsoft, Disney, Infoseek) stopped accepting advertising on their websites from sites that do not post privacy policies

Rights and Law

- Legal protections for personal data collected or used by other people, businesses, and organizations
  - Until the late 19th century, no recognition of an independent right to privacy
  - courts based their decisions on property rights and contracts
- Warren and Brandeis (1890): *The inviolate personality*
  - criticism of newspaper gossip columns that
  - people have the right to prohibit publication of facts about themselves and photographs of themselves
    - privacy is distinct and needs its own protection

Rights and Law

- Judith Jarvis Thomson (philosopher, 1929-):
  - Is there a right to privacy?
    - Argues that other rights and laws protect privacy
- Transactions
  - Privacy includes control of information about oneself
  - But, several people participate in transactions
  - Example: Joe buys five pounds of potatoes from Maria
    - Joe asks for confidentiality as part of the transaction
      - Maria has three options
      - (1) She can agree.
      - (2) She can say no; she might want to tell people she sold potatoes to Joe.
      - (3) She can agree to keep the sale confidential if Joe pays a higher price
  - If the agreement is a legal contract, then they have a legal obligation to respect it.

Rights and Law

- Ownership of personal data
  - Who is the owner of personal information?
    - assigning ownership of personal information arises from the notion of owning facts
    - Do you own your birthday or your mother owns it? She participated more in it.
  - Judge Richard Posner (7th circuit, Chicago)
    - allocate property rights to information
- A basic legal framework:
  - Enforcement of agreements and contracts
    - Example: Toysmart, a Web-based seller of educational toys, collected extensive information on about 250,000 visitors (promised not to release this personal information in the contract)
      - When it applied for bankruptcy, creditors posted the database for sale
      - the bankruptcy-court settlement included destruction of the database

Rights and Law: Contrasting viewpoints

- Free Market View
  - Freedom of consumers to make voluntary agreements
  - Diversity of individual tastes and values
  - Response of the market to consumer preferences
  - Voluntary organizations that provide consumer education
  - Usefulness of contracts
  - Flaws of regulatory solutions
- Consumer Protection View
  - More stringent requirements, prohibitions on businesses of storing or selling certain type of data
  - Protect consumers against collection or storage of information that they don't understand
    - because personal information leaks out
  - Consumers need protection from their own lack of knowledge, judgment, or interest
    - consumers may not understand the uses of their health information

Rights and Law: Contrasting viewpoints

- Consumer Protection View
  - Individuals have no meaningful power against large companies like Google and Apple
  - Consumer pressure is sometimes effective, but some companies ignore it.
  - Must require all businesses to adopt pro-privacy policies

Privacy Regulations in the European Union

- EU's rules are more strict than U.S. regulations
- EU Data Privacy Directive (1995)
  - Prohibits transfer of personal information to countries outside the EU that do not have an adequate system of privacy protection.
  - Processing of data is permitted only if the person has consented unambiguously or if the processing is necessary to fulfill contractual or legal obligations or is needed for tasks in the public interest or by official authorities to accomplish their tasks
  - "Safe Harbor" plan
    - EU agreed to the "Safe Harbor" plan, under which companies outside the EU that agree to abide by a set of privacy requirements similar to the principles in the Data Protection Directive may receive personal data from the EU

2.6 Communications

- Wiretapping and Email Protection
  - Law enforcing may intercept communications for national security
  - Telephone
    - In 1928, the Supreme Court ruled that wiretapping by law enforcement agencies was not unconstitutional
    - 1934 Communications Act prohibited interception of messages
      - there is no exception for law enforcement agencies
    - Law enforcement agencies continued to wiretap regularly for decades, sometimes with the approval of the U.S. Attorney General
    - 1968 Omnibus Crime Control and Safe Streets Act allowed wiretapping and electronic surveillance by law-enforcement (with court order)
  - Email and other new communications
    - Electronic Communications Privacy Act of 1986 (ECPA) extended the 1968 wiretapping laws to include electronic communications, restricts government access to email

Communications

- The government argued that people give up their expectation of privacy by allowing ISPs to store their email on the ISP's computers
  - A federal appeals court ruled that people do have an expectation of privacy for email stored at their ISP and that police need a search warrant to get it
- Designing Communications Systems for Interception
  - The Communications Assistance for Law Enforcement Act (CALEA)
    - Passed in 1994
    - Requires telecommunications equipment be designed to ensure that the government can intercept telephone calls (with a court order or other authorization).
    - Rules and requirements written by Federal Communications Commission (FCC)
    - BlackBerry were required to provide access to governments to personal data

The NSA and Secret Intelligence Gathering

- The National Security Agency (NSA)
  - A secret presidential order formed the NSA in 1952
  - NSA monitored communications of specific American citizens (including civil rights leader Martin Luther King Jr. and entertainers who opposed the Vietnam War)
  - Foreign Intelligence Surveillance Act (FISA, 1978) established oversight rules for the NSA
  - Secret access to communications records, purchases
    - In 2006, it leaked that NSA set up at an AT&T switching facility
  - Also monitors other governments (not only hostile governments)
  - Congress passed the FISA Amendments Act in 2008
    - protects AT&T and other ISPs from lawsuits