Computer Law and Ethics, COSC-3325, Lecture 2

Stefan Andrei

Reminder of the last lecture

- Rapid Pace of Change
- New Developments and Dramatic Impacts
- Issues and Themes
- Ethics

Overview of This Lecture

- Privacy and Computer Technology
- “Big Brother is Watching You”
- Privacy Topics
- Protecting Privacy
- Communications

Context of privacy

- Surveillance cameras watched shoppers in banks and stores.
- Private investigators still search household garbage for medical and financial information, purchases, notes, and so on.
- Computer technology is not necessary for the invasion of privacy.
- However, computer and Internet made new threats possible and old threats even more potent.

Privacy and Computer Technology

- There are three key aspects of privacy:
  1. Freedom from intrusion (being left alone);
  2. Control of information about oneself;
  3. Freedom from surveillance (being tracked, followed, watched).
- Clearly, we cannot expect complete privacy.
- Living in a small town has less privacy, while in a big town we may be anonymous.

Personal information

- Includes information about an individual person.
- It is in general associated with that person's "handle", such as, user name, online nickname, identification number, or e-mail address.
- It can also be extended to non-alpha-numeric data, such as, personal images.

Categories of privacy threats

1. Intentional, institutional uses of personal information (e.g., law enforcement, tax collection, and so on);
2. Unauthorized use/release by "insiders" (people who maintain the information);
3. Theft of information;
4. Inadvertent leakage of information through negligence;
5. Personal actions (intentional or unaware of the risks).

Privacy and Computer Technology (cont.)

New Technology, New Risks:

- Government and private databases;
  - These databases may contain outdated data;
  - Records of different people with similar names get confused.
- Sophisticated tools for surveillance and data analysis (tiny cameras in cell phones);
- Vulnerability of data (emails can be forwarded to many people).

Privacy and Computer Technology (cont.)

Terminology:

- Invisible information gathering - collection of personal information about someone **without** the person's knowledge;
- **Example:** cookies are files that a web site stores on each visitor's computer.
  - A retail store might store information about products we looked at and our virtual shopping cart.
  - On subsequent visits, the site retrieves information from the cookie and uses for market purposes.

Privacy and Computer Technology (cont.)

Terminology:

- Secondary use - use of personal information for a purpose other than the one it was provided for.
- **Examples:**
  - Sale of customer information to marketers
  - Use of information in various databases to deny someone a job
  - Use a supermarket's customer database to show alcohol purchases by a man who sued the store because he fell down.

Privacy and Computer Technology (cont.)

Terminology (cont.):

- Data mining - searching and analyzing masses of data to find patterns and develop new information or knowledge;
- Computer matching - combining and comparing information from different databases (using social security number, for example, to match records).
- Example: businesses use data mining and computer matching to find new customers.

Privacy and Computer Technology (cont.)

Terminology (cont.):

- Computer profiling - analyzing data in computer files to determine characteristics of people most likely to engage in certain behavior.
- Example: government agencies use computer profiling to identify people to watch or find suspects for some activities.

Privacy and Computer Technology (cont.)

Principles for Data Collection and Use:

1. Informed consent;
2. Opt-in and opt-out policies;
3. Fair Information Principles (or Practices);
4. Data retention.

Principle 1. Informed consent

- When people are informed about the data collection and use policies of a business or organization, they can decide whether or not to interact with that business or organization.
- Examples:
  - Some people post personal profiles and videos displaying their personal lives and emotions to world;
  - Some other people use cash to avoid leaving a record of their purchases, encrypt all their emails, use anonymizers to hide their identity when surfing the web, and very angry when information is collected about them.

Principle 2. Opt-out and opt-in policies

- After informing people what an organization does with personal information, the next desirable policy is to give people some control over secondary uses.
  - Opt-out policy: one must check/click a box on a contract to request that his/her information not to be used in a particular way. Otherwise, the presumption is that the organization may use his/her information may be used.
  - Opt-in policy: the collector of the information may not use it for other purposes unless the consumer explicitly checks/clicks a box permitting the use.
- Note: do not confuse opt-out and opt-in policies.
  - Under opt-out, more people are likely to be 'in' (their information will be used), while for opt-in, more people are likely to be 'out'.
  - The assumption in opt-out is that you agree with them, while for opt-in, the assumption is that you don't agree.

Principle 3. Fair Information Practices

- Some companies and organizations turn over personal data to law enforcement agents and government agencies when requested.
- Some do so only if presented with a subpoena or other court order.
- Some challenge subpoena, others don't.
- Some inform their customers or members when they give personal data to the government, others don't.
- The entity that holds the data decide how far to go to protect the privacy of its customers or members.

Principle 4. Data retention

- Large databases of businesses and government have the following principles:
  1. Inform people when identifiable information are collected and how it will be used;
  2. Collect only the data needed;
  3. Offer ways to opt out from mailing lists, advertising, transfer of their data, etc;
  4. Provide stronger protection for sensitive data (e.g., an opt-in policy for disclosure of medical data);
  5. Keep data only as long as needed;
  6. Maintain accuracy of data;
  7. Provide security of data (from theft or leaks).

Privacy and Computer Technology Discussion Questions

- Have you seen opt-in and opt-out choices? Where? How were they worded?
- Were any of them deceptive?
- What are some common elements of privacy policies you have read?

"Big Brother (the Government) is Watching You"

Here are the topics related to the government's databases:

- The Government Accountability Office (GAO) - monitors government's privacy policies
- Burden of proof and "fishing expeditions" due to computer technologies
- Data mining and computer matching to fight terrorism

Government's privacy policies

- Federal and local government agencies have databases with personal data, that are required to be reported from businesses:
  - Tax records
  - Medical records
  - Marriage and divorce records
  - Property ownership
  - Welfare records
  - School records
  - Motor vehicle records
  - Voter registration records
  - Applications for government grant and loans, and so on.

Government's privacy policies

- GAO is Congress's "watchdog agency" for monitoring the government's privacy policies.
- **Example 1:** A major GAO study, released in 1996, describes how Congress investigated a "secret" database that the White House maintained on 200,000 people with more than a hundred fields of data for each person, including ethnic and political information.
- **Example 2:** A GAO study of 65 government Web sites in 2000 found that only 3% of the Web sites fully complied with the fair information standards for notice, choice, access, and security established by the Federal Trade Commission (FTC) commercial Web sites.
- **Example 3:** In 2005, the GAO reported that IRS used data mining to detect fraud that did not comply with all rules for collecting information on citizens.

Burden of proof and "fishing expeditions"

- Computer technologies have altered the nature of tax, criminal, and other government investigations.
- Instead of collecting evidence from a variety of sources, the modern techniques can search huge volumes of information, seeking people who look suspicious.
- Cons: In many cases, a presumption of guilt replaces the traditional presumption of innocence.
- Pro: Databases and search technologies help the law enforcement agencies to easily find an answer.

Data mining and computer matching to fight terrorism

- Before September 11, 2001, law enforcement agencies lobbied for increased powers that conflicted with privacy.
- Example 1. Congress passed a strong privacy protection law – people resisted privacy intrusion by government.
- After that date, people became willing to accept uses of personal data and surveillance.
- Example 2. CAPPS (Computer Assisted Passenger Prescreening System) gave government access to passenger information in airline databases.
- Example 3. CAPPS II and Total Information Awareness were not approved due to intense opposition.

Discussion Questions about the personal data use or data mining

- Is the information it uses or collects accurate and useful?
- Will less intrusive means accomplish a similar result?
- Will the system inconvenience ordinary people while being easy for terrorists to thwart?
- How significant are the risks to innocent people?

"Big Brother is Watching You" (cont.)

- 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."*

Expectation of Privacy and Surveillance Technologies

- The Fourth Amendment weakened because:
  1. Much of our personal information is no longer safe in our homes;
  2. New technologies allow the government to search our homes without entering them.
- Supreme Court uses the notions of expectation of privacy to determine their decisions
  - Modern surveillance techniques are redefining expectation of privacy, such as automated toll collection and itemized purchase records.

"Big Brother is Watching You" (cont.)

- The USA PATRIOT Act and other antiterrorism laws have many controversial provisions, such as:
- The USA PATRIOT Act and National Security Letters (NSL):
  - Before September 11, NSLs (investigation without court order or court oversight needed) were issued only with approval from an FBI headquarters official.
  - After September 11, the PATRIOT Act expanded FBI authority so that any FBI agent can issue NSL.
  - 2003-2005 report found that 143,000 NSLs were issued.
  - This was considered a "widespread and serious misuse" of the FBIs national security letter authorities.

"Big Brother is Watching You" (cont.)

Video Surveillance:

- Security cameras: increased security, but decreased privacy
- We are used to cameras in banks and stores.
- They exist in gambling casinos, traffic lights intersections, and so on.
- After September 11, Washington D.C. police installed cameras which can recognize individuals half a mile away.
- Cameras combined with face recognition raise some relevant privacy and civil liberties issues.

Example of a camera computer system

- In Tampa, Florida police scanned 100,000 fans and employees who entered the 2001 Super Bowl.
- People were not told that their faces were scanned.
- In over two years of using the system, the police didn't recognize anyone they were looking for, but it did occasionally identify innocent people as wanted felons.
- However, some applications of face-recognition cameras are reasonable and beneficial for crime prevention.

"Big Brother is Watching You" (cont.) Discussion Questions

- What data does the government have about you?
- Who has access to the data?
- How is your data protected?

Diverse Privacy Topics

Marketing is an essential task for most businesses and organizations.

- Targeted marketing means to identify the people interested in your products or services.
  - Data mining
  - Paying for consumer information
  - Data firms and consumer profiles
  - **Example:** The store customer card are given us based on voluntarily agreement. However, some stores may used what products we buy and change the item's prices to maximize profit.
- Credit records: credit companies sell mailing lists based on credit information to other businesses.

Diverse Privacy Topics (cont.)

Location Tracking:

- Global Positioning Systems (GPS)
  - computer or communication services that know exactly where a person is at a particular time
  - it can also reveal the previous destinations, even if don't want that.
- Cell phones and other devices are used for location tracking
- Pros and cons

Radio-Frequency IDentification (RFID) tags

- Are small devices that contain a computer chip and an antenna.
- The chip stores identification data and controls operations of the tag.
- RFID tags are inserted in many products to track them through the manufacturing and selling processes.
- If not disabled after a customer buys the product, the tag can be used for tracking that person.

Diverse Privacy Topics (cont.)

Stolen and Lost Data:

1. Hackers
2. Physical theft (laptops, thumb-drives, etc.)
3. Requesting information under false pretenses
4. Bribery of employees who have access

- Except for hackers, these are not new to computer technology.
- Before computers, files were stolen, receipts were stolen, information was requested under false pretenses and employees were bribed.
- But, with computers, the extent and impact have grown.

Diverse Privacy Topics (cont.)

What We Do Ourselves:

- Many people publish personal information in blogs and online profiles, including pictures of their families.
- A viable solution would be to give access only to whose users who register to that website.
- File sharing and storing: several medical websites allow people to store their medical records online.
- Is privacy old-fashioned?
  - Young people put less value on privacy than previous generations.
  - They may not understand the risks.

Diverse Privacy Topics (cont.)

Public Records: Access vs. Privacy:

- Public Records mean records available to general public (bankruptcy, property, and arrest records, salaries of government employees, etc.)
- Identity theft can arise when public records are accessed.
- How should we control access to sensitive public records?
- Under the old rules for the financial statements of judges, people requesting access had to sign a form disclosing their identity.
- It is not simple to implement this rule online.

Diverse Privacy Topics (cont.)

National ID System:

- Social Security Numbers were invented in 1936 for the Social Security program.
- Later, in 1943, President Roosevelt required agencies to use SSNs for new record systems.
- In 1961, the IRS uses SSN as a tax payer ID number.
- Many people believe SSNs are too widely used and they are easy to falsify.

Diverse Privacy Topics (cont.)

National ID System (Cont.):

- A new national ID system - Pros
  - would require the card
  - harder to forge
  - have to carry only one card
- A new national ID system - Cons
  - Threat to freedom and privacy
  - Increased potential for abuse

Diverse Privacy Topics (cont.)

Children:

- The Internet
  - Not able to make decisions on when to provide information
  - Vulnerable to online predators
- Parental monitoring
  - Software to monitor Web usage
  - Web cams to monitor children while parents are at work
  - GPS tracking via cell phones or RFID

Diverse Privacy Topics Discussion Questions

- Is there information that you have posted to the Web that you later removed? Why did you remove it? Were there consequences to posting the information?
- Have you seen information that others have posted about themselves that you would not reveal about yourself?

Protecting Privacy

Technology and Markets:

- Many individuals and businesses help meet the demand for privacy to some degree.
- Organizations such as the Privacy Rights Clearinghouse provide excellent information resources.
- New applications of enhancing-technologies for consumers often can solve problems that arise as side effects of technology.
- Encryption is such as important technological tool for protecting privacy.
- Privacy Rights Clearinghouse is a non-profit consumer education and advocacy project whose purpose is to advocate for consumers' privacy rights in public policy proceedings. Official website: www.privacyrights.com

Tools for protecting data

- Public-key cryptography represents a safe way of encryption that allows communication between two agents without knowing the key in advance.
- There exist business tools and policies for protecting data.
- A well-designed database for sensitive information includes authorized username and password.
- The computer keeps track of all accesses, including ID of the person looking for information.

Protecting Privacy (cont.)

- The Fourth Amendment protects the negative right (a liberty) against intrusion by government.
- We describe now the rights and laws regarding protecting data collected or used by other people, businesses, and organizations.
- There exist two main theories:
  - Warren and Brandeis
  - Thomson

Warren and Brandeis's Theory

- *People have the right to prohibit publication of facts or photographs about themselves;*
- Example: *If someone writes a letter describing a fight with his wife, that fact is protected and cannot be published by the recipient of the letter*.
- Privacy is distinct from other rights, hence it needs its own protection.
- Critics said their theory violates the freedom of the press.

Thompson's Theory

- *Suppose you own a magazine.*
- *Your property rights include the right to refuse to allow others to read, destroy, or even see your magazine.*
- *If someone does anything to your magazine that you didn't allow, that person is violating your privacy rights.*
- Critics of Thompson said her theory is too vague … it holds only for a finite number of examples.

Transactions

- It is complicated to apply philosophical and legal notions of privacy to transactions, which automatically involve more than one person.
- The parties involved in the transaction should agree which parts should be kept confidential (the price per item, the entire amount, the identity of the buyer and seller, and so on).

Ownership of personal data

- Some economists, legal scholars, and privacy advocates propose giving people property rights in information about themselves.
- Example 1: Do we own our birthday? Or the mother? After all, she was a more active participant in the event!
- Example 2: Copyright protects intellectual property such as computer programs and music, but we cannot copyright facts.
- Example 3: We cannot own the fact that our eyes are blue, but we do have the legal right to control some uses of our photographic image.

Regulation

- Technical tools for privacy protection are not perfect.
- Some privacy advocates consider this a strong argument for regulatory laws.
- Regulation is not perfect either.
- Example of a privacy law: After years of controversy, the federal government issued comprehensive medical privacy regulations under the Health Insurance Portability and Accountability Act (HIPAA) in 2003.
  - Medical insurers now must not disclose patient medical records to lenders, employers, and marketers without the patient's consent.

Contrasting Viewpoints:

- When asked “If someone sues you and loses, should they have to pay your legal expenses?”, more than 80% of surveyed people said “yes”.
- When asked the same question from the opposite perspective “If you sue someone and lose, should you have to pay their legal expenses?”, only 40% said “yes”.

Protecting Privacy (cont.)

Rights and laws:

- A free market economy is an economy based on the power of division of labor in which the prices of goods and services are determined in a free price system set by supply and demand.
- Free Market View:
  - Freedom of consumers to make voluntary agreements
  - Diversity of individual tastes and values
  - Response of the market to consumer preferences
  - Usefulness of contracts
  - Flaws of regulatory solutions

Protecting Privacy (cont.)

- Organizations collecting personal data should clearly inform the person providing the information if they will not keep it confidential (from other businesses, individuals and government agencies) and how they will use it.
- The market viewpoint respects the right and ability of consumers to make choices for themselves based on their own values.
- Example: we cannot always expect exactly the mix of attributes we want in any product or service.
  - For instance, just as we might not be able to find a car with the exact set of features we want, we might not be able to get both privacy and special discounts.

Protecting Privacy (cont.)

Rights and laws: Contrasting Viewpoints (cont.):

- Consumer protection laws are designed to ensure fair trade competition and the free flow of truthful information in the marketplace.
- The consumer-protection view is to protect consumers against abuses and carelessness by businesses and against their own lack of knowledge.

Protecting Privacy (cont.)

- Consumer Protection View
  - Uses of personal information
  - Costly and disruptive results of errors in databases
  - Ease with which personal information leaks out
  - Consumers need protection from their own lack of knowledge, judgment, or interest
- The consumer-protection viewpoint sees privacy as a right rather than something we bargain about.
- Positive right: we can stop others communicating about us.
- Negative right: we can use technology to refrain from interacting with those who request information we don't wish to provide.

Protecting Privacy: European Union

- European Union (EU) has a comprehensive Data Protection Directive covering processing of personal data, collection, use, storage, retrieval, transmission, destruction, and others.
- It is more strict than U.S. regulations, but abuses still occur.
- The EU agreed to abide by a set of privacy requirements for the companies outside the EU similar with their Data Protection Directive.
- Example: after 2001, screening of air travel passengers from Europe to the U.S. raised problems because the U.S. wanted more information about the travelers.

Protecting Privacy
Discussion Question

- How would the free-market view and the consumer protection view differ on errors in Credit Bureau databases?
- Who is the consumer in this situation?

Communication

- Law enforcement agencies intercept communications to collect evidence of criminal activities.
- Intelligence agencies intercept communications to collect information about activities and plans of hostile governments and terrorists.
- The Fourth Amendment to the U.S. Constitution and other laws put restrains on their activities in order to protect innocent people and reduce the opportunity for abuses.

Communication (cont)

Wiretapping and E-mail Protection:

- Within ten years of the invention of the telephone (1920), people were wiretapping them [Baa08].
- The legal status of wiretapping was debated throughout most of the 20th-century.
- Telephone:
  - 1934 Communications Act prohibited interception of messages
  - 1968 Omnibus Crime Control and Safe Streets Act allowed wiretapping and electronic surveillance by law-enforcement (with court order)

E-mail and other new communications

- Old laws did not explicitly cover e-mail and cell phone conversation, and interceptions were common when e-mail and cell phones were new.
- Electronic Communications Privacy Act of 1986 (ECPA) extended the 1968 wiretapping laws to include electronic communications, restricts government access to e-mail
- Other systems: The meaning of pen register has changed over time. It originally referred to a device that recorded the numbers called from a phone. Now it also refers to logs phone companies keep of all numbers called, including time and duration.

Communication (cont.)

- New communications technologies developed in the 1980s and 1990s made access to the content of telephone calls more difficult for law enforcement agencies than it was before.
- Intercepting Internet phone calls is more difficult than attaching a clip to an old analog telephone wire.

Communication (cont.)

- FBI helped draft the Communications Assistance for Law Enforcement Act of 1994 (CALEA):
  - Telecommunications equipment must be designed to ensure government can intercept telephone calls;
  - Rules and requirements written by Federal Communications Commission (FCC).
  - The essential argument in favor of CALEA is to maintain the ability of law enforcement agencies to protect us from drug dealers, organized crimes, other criminals, and terrorists in a changing technological environment [Baa08].

Communication (cont.)

Secret Intelligence Gathering:

- The National Security Agency (NSA) collects and analyses foreign intelligence information related to national security.
- There were some secret accesses to communications records.
- In order to monitor NSA, the Congress passed the Foreign Intelligence Surveillance Act (FISA) who established oversight rules for the NSA.

Wiretapping

- All wiretapping of American citizens by the NSA requires a warrant from a three-judge court set up under the FISA.
- After 2001, Congress passed the Patriot Act, which granted the President broad powers to fight a war against terrorism.
- The administration used these powers to bypass the FISA court and directed the NSA to spy directly on terrorist groups in a new NSA electronic surveillance program.
- Reports at the time indicate that an "apparently accidental" glitch resulted in the interception of communications that were purely domestic in nature.

Wiretapping (cont)

- The New York Times disclosed that since 2002, the NSA was intercepting international phone calls and e-mails of several hundred or several thousand people in the U.S.
- This action was challenged by a number of groups, including Congress, as unconstitutional.
- Supporters of the program argued that the NSA must be able to quickly monitor communications to protect the U.S. from a terrorist attack was essential [Baa08].
- About a year after disclosure of the program, the government agreed to stop warrantless wiretapping and submit the terrorism-related wiretap requests to the FISA court.

Communication (cont.)

Encryption Policy:

- For decades, most of the cryptographers in the U.S. worked for the NSA.
- The NSA almost certainly could break virtually any codes that were in use before the mid-1970s.
- Government ban on export of strong encryption software in the 1990s (removed in 2000).
- As a consequence, encryption products produced by U.S. companies for export were less competitive than those of foreign companies that used better encryption techniques.

The National Research Council study

- In 1996, a panel of experts from business, government, and academia prepared a study of encryption policy for the National Research Council (NRC).
- The study strongly supported the use of powerful encryption.
  - The government appeared to have ignored the NRC report.
  - The U.S. policy was strangely outdated and all stronger encryption schemes were available on Internet sites all over the world.

Philip R. Zimmermann

- … is the creator of Pretty Good Privacy, an email encryption software package.
- Originally designed as a human rights tool, PGP was published for free on the Internet in 1991.
- This made Zimmermann the target of a three-year criminal investigation, because the government held that U.S. export restrictions for cryptographic software were violated when PGP spread worldwide.
- Despite the lack of funding, the lack of any paid staff, the lack of a company to stand behind it, and despite government persecution, PGP nonetheless became the most widely used email encryption software in the world.

Philip R. Zimmermann (cont)

- After the government dropped its case in early 1996, Zimmermann founded PGP Inc.
- That company was acquired by Network Associates Inc. (NAI) in 1997, where he stayed on for three years as a Senior Fellow.
- In 2002 PGP was acquired from NAI by a new company called PGP Corporation, where Zimmermann served as special advisor and consultant until its acquisition by Semantec in 2010.
- Zimmermann currently is consulting for a number of companies and industry organizations on matters cryptographic.

Communication Discussion Questions

- What types of communication exist today that did not exist in 1968 when wiretapping was finally approved for law-enforcement agencies?
- What type of electronic communications do you use on a regular basis?

Summary

- Privacy and Computer Technology
- “Big Brother is Watching You”
- Privacy Topics
- Protecting Privacy
- Communications

Reading suggestions

- From [Baase; 2007]
  - Chapter 2

Coming up next

- How Pretty Good Privacy (PGP) works?
  - This lecture is inspired from Chapter 1 of the *Introduction to Cryptography* in the PGP 6.5.1 documentation. Copyright © 1990-1999 Network Associates, Inc. and its Affiliated Companies.
    - Available online at http://www.pgpi.org/doc/pgpintro/, accessed on January 2, 2011
    -

Thank you for your attention!

Questions?