Social Implications of a Computerized Society

Chapter 2: Privacy

Instructor: Oliver Schulte

Simon Fraser University

Outline

- Privacy and Computer Technology
- Privacy and Businesses
- Privacy and the Government
- Protecting Privacy
  - Technology
  - Markets
  - Law
  - Theory

Key Concepts and Issues

- Informed Consent
- Reasonable Expectation of Privacy
- Control of Information
- Secondary Use
- Computer Profiling
- Invisible Information Gathering
- New Dangers to Privacy
- Privacy Protection Methods

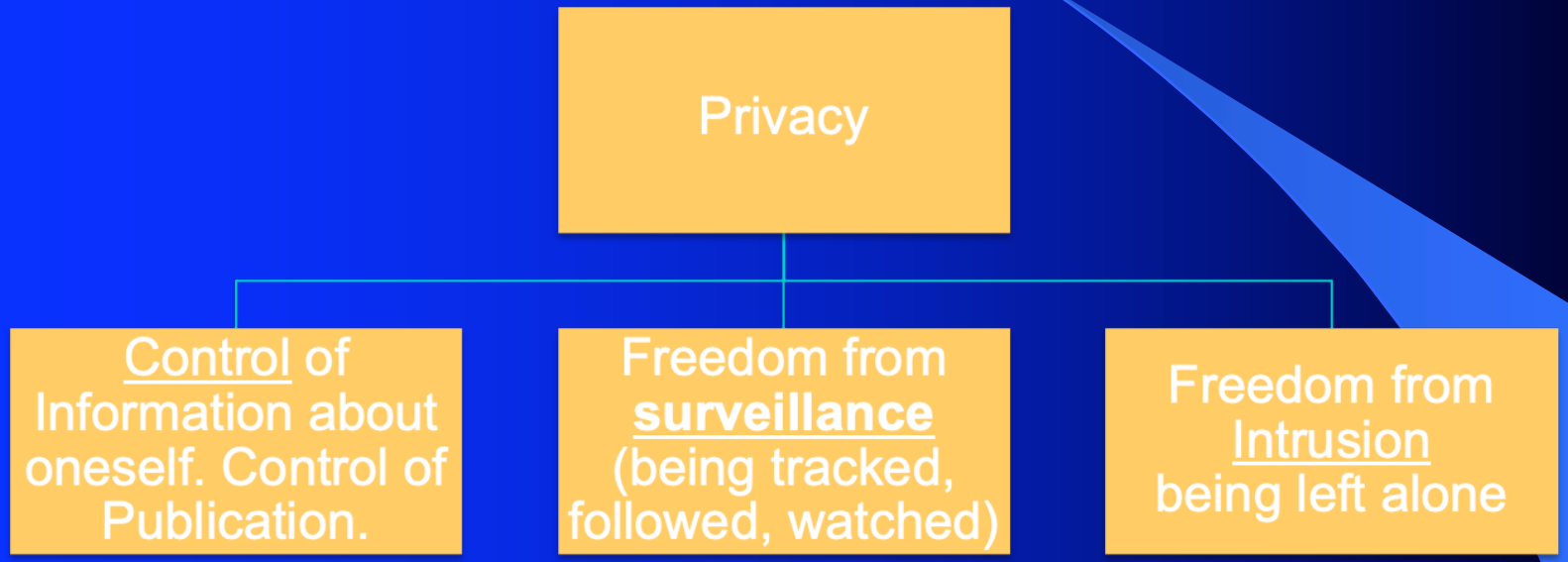
Group Discussion Questions

Take canvas survey “Privacy”

1. Have you experienced an invasion of privacy yourself that was due to computer technology? Can you propose a (feasible and reasonable) rule/law/technology that would prevent this problem?
2. Have you ever traded personal information/privacy for a benefit? What trade-offs would you be willing to make yourself? What should be the rules about trading personal information for everyone?

Basic Privacy Concepts

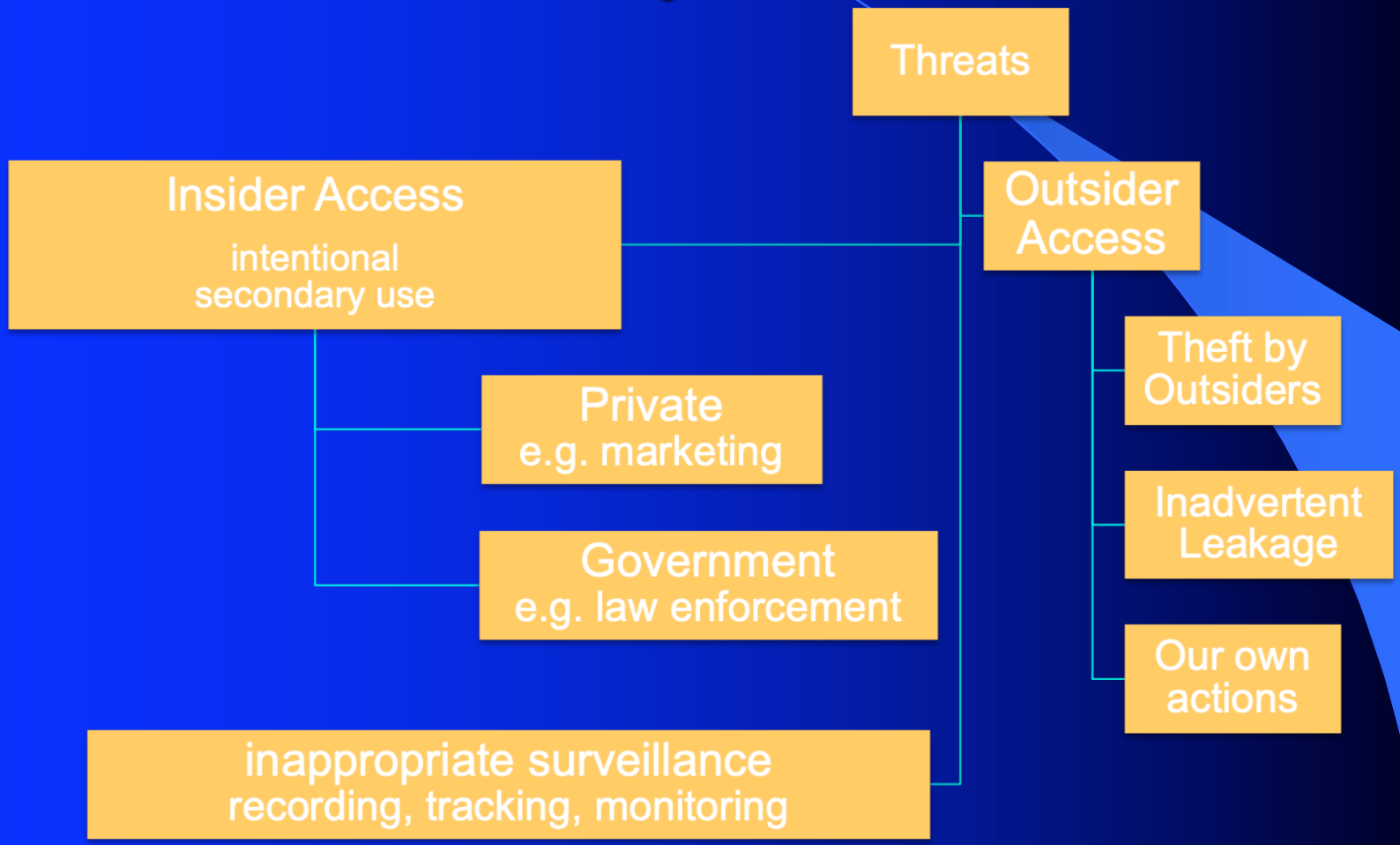
What Is Privacy?



"It's important to realize that privacy preserves not personal secrets, but a sense of safety within a circle of friends" Robert Ellis Smith

"Privacy in group association may be indispensable to ... freedom of association." U.S. Supreme Court

Privacy Threats



Privacy Terminology I

- **Invisible information gathering** - collection of personal information about someone without the person's knowledge
- **Secondary use** - use of personal information for a purpose other than the one it was provided for

Privacy Terminology II

- **Data mining** - searching and analyzing masses of data to find statistical patterns and develop new information or knowledge
- **Computer matching** - combining and comparing information from different databases (using social insurance number, for example, to match records)

Privacy Terminology III

- **Computer profiling** - analyzing data in computer files to determine characteristics of people most likely to engage in certain behavior
  - Business: find likely customers.
  - Police: find likely criminals.
- **Fishing expeditions**: gather data from people without evidence of guilt ("probable cause")

Privacy Threats and Computer Technology

Privacy Threats and Computer Technology: Secondary Uses

Computer technology has added new threats and new dimensions

- Large databases covering millions of people enable
  - data mining
  - profiling
- data sharing
- data “fishing expeditions”

Privacy Threats and Computer Technology: Outside Access

Computers have added new threats and new dimensions

- Data in the cloud is vulnerable to hacking
- Once on the web, permanent public record

Privacy Threats and Computer Technology: Surveillance

Computers have added new threats and new dimensions

- Invisible information gathering
  - e.g. spyware, web browsers
- video recording
- cell phone location tracking (stingrays)

Privacy Principles

Group Discussion

What are good principles and rules for countering privacy threats (both for government and for business). Do you think they are observed already?

1. For secondary information uses by insiders
2. For data security (unauthorized data access)
3. For (invisible) information gathering

Fair information principles

- Inform people
  - when you collect information.
  - what you collect
  - how you use it
- Collect only the data needed.
- Offer a way for people to opt out from mailing lists, advertising, services.
- Keep data only as long as needed.
- Maintain accuracy and security of data.
- Develop and publish policies for responding to law enforcement requests for data.

Privacy Threat Examples

Privacy Doctor

- Diagnosis: what went wrong
- Prescription: how to prevent another occurrence

Information theft

Stolen and Lost Data

Data Theft Methods

- Hacking
- Physical theft (laptops, thumb-drives, etc.)
- Requesting information under false pretenses
- Bribery of employees who have access.

Data Breaches Occur Regularly

- Have you been pwned?
- Files on hundreds of thousands of university students were stolen by hackers
- Contact information for more than 1M job seekers stolen from Monster.com
- Names, SINs, addresses stolen from laptop in hospital employee's car
- Solarwind data breach
- Uber Data Breach
- Morgan Stanley Data Breach: stolen then hacked
- Ashley Morgan Data Breach
- Cambridge Analytica Data Breach
  Facebook allowed a 3rd-party app to access users' personal information
- U.S. government officials sold data to credit card fraud ring, collection agencies
- Current allegations against Amazon employees

Diagnosis

Which fair information principles were violated?

- Protect security of data
- Perhaps kept data for too long

Prescription: Solutions

- encryption for sensitive data
- disallow local storage (laptop)
- access control against hacking, 3rd-party apps
- track and log access (against data sale)
  - support **privacy audits**

Businesses

Secondary Data Uses

Marketing and Personalization

Consumer Dossiers:

- Targeted marketing/ads
  - Data mining
  - Paying for consumer information
  - Data firms and consumer profiles
  - Henry Ford: "I know half of my advertising budget is wasted. I just don't know which half."
- Credit records

Secondary Use Example

- Credit card companies sell name and information for targeted marketing.
- Some charities sell donor information to mail and phone lists
- British Tesco (grocery) found that young men who buy diapers also buy beer -> mails out coupons.
- U.S. Target (retail) analyzed buying patterns to predict pregnancies – sometimes before the families know!
- Game apps for children pass location, ages, genders to advertising companies
  - violates Children's Online Privacy Protection Act (COPPA)

Web Searches

- Google uses your activity history to target ads for searches and Gmail
- Also provides information to law enforcement.
- How long does Google keep your activity records? Forever?
- In 2006, the Bush admin asked Google to hand over search data in defense of an Internet pornography law. Google fought and won in court.
- There are also private search engines like DuckDuckGo

Social Media

- Facebook issues:
  - automatically tagging people in photos
  - reposting purchase information to friends (the Beacon program)
  - leaking location check-ins to the network

- Lesson: The easier the access to information, the worse the loss of control
- Push is worse than pull

Diagnosis

- Informed Consent was not observed.
- Information about data use missing in business contracts/service terms
- Better in Google
- Consent not obtained by Facebook (can you opt out of Newsfeed?)

Prescription – Solutions

- Inform about secondary uses like targeting, marketing
  - e.g., you may receive marketing material based on purchase behavior
- Provide opt-out options.
- Consider opt-in options, like for advertisting purchases (e.g. for NewsFeed)

Discussion Questions

Consider secondary uses like

- marketing
- tracking
- access personal information by 3rd parties (apps)
- Which of these should be subject to opt-out or opt-in conditions?

Government

Secondary data uses

Government vs. Business Data Collection

- Business must offer customers something in return for their data
  - except for invisible information gathering.
- Governments can force people to provide personal information (e.g. tax return, medical records)
- ➢ arguably governments have an even greater responsibility to protect information
- also a greater responsibility to keep information accurate (more later)

Examples

- Every year hundreds of IRS (US tax agency) employees are investigated for snooping in tax returns
- IRS scans vehicle registration records to find people with expensive cars and boats.
- State department employees opened Barack Obama's passport file

Fishing Expeditions and Computer Matching

- Traditionally, crime happens first, then suspects are sought.
- In fishing expeditions, gvt scans information to look for suspicious activity or people.
- Examples:
  - satellite photos to catch people building backyard porches without permits.
  - tax agency IRS scans vehicle registration records
  - During Vietnam war, Secret Service bought birthday list from ice cream chain to find 18-year olds who had not registered for the draft.
  - also illustrates government use of private sector sources

Discussion Questions

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

Examples of government databases

- U.S. SORNS
- https://www.dhs.gov/system-records-notices-sorns
- You can find out what information the government has collected about you by an Access to Information request (ATI)

Privacy Law

General Comment on Case Law

- England and its former colonies use a legal system known as case law.
- Law makers (parliament) pass laws with general principles and somewhat vague language.
- When cases are brought to court, judges rule on details for applying the law (e.g. Katz vs. United States)

Case Law vs. Positive Law

- Positive law is an alternative approach.
- Law makers write rules that cover as many specific situations as possible.
  - Roman law, Napoleonic code, most European countries other than U.K.
- Case law can be easier to adapt to new technologies

Data Breaches

- Companies must protect personal information
- Liable to fines and law suits for damages
  - e.g. Ashley Madison case
- strict new EU regulations

Legal Perspective

Secondary Uses

Informed Consent

- Companies must inform users about secondary uses and obtain their consent.
- Consistent with a free market viewpoint:
  - users freely trade personal information for IT benefits

Informed Consent: Discussion Questions

- How much information is required?
  - is it enough to say “agree to our privacy policy”
  - how easy should it be for users to view/correct the information stored (e.g. google activity)?
- what counts as consent?
  - agree once?
  - Opt-out?
  - Opt-in for every secondary use (e.g. advertise purchase on facebook?)

Legal perspective

surveillance

My Home is My Castle

- Strong Anglo tradition for physical privacy in the home

=

Prime Minister Pitt in 1763:
"The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake: ... the storms may enter; the rain may enter—but the Kind of England cannot enter"

U.S. Constitution and CDN Charter

- Amendment 4: 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.
- CDN Charter: **8.** Everyone has the right to be secure against unreasonable search or seizure.

Surveillance = Search

- Obtaining private personal information has been treated by the law as analogous to a physical search.
- Examples:
  - thermal imaging of homes
  - stringrays for phone tracking
  - intercepting communications, wiretap

Communication Privacy

Wiretapping and E-mail Protection: - see SciAm diagram.

- 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).
  - 2009 decision: international call tapping without warrant ok.
- E-mail and other new communications
  - Electronic Communications Privacy Act of 1986 (ECPA) extended the 1968 wiretapping laws to include electronic communications, restricts government access to e-mail

Designing Communications Systems for Interception

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)
- Example: The Clipper Chip

Secret Intelligence Gathering

- The National Security Agency (NSA) analyze foreign intelligence communication outside the U.S.
- Secret access to communications records
- But what about Americans communicating with foreigners?
  - Example of **transactional privacy**
  - Foreign Intelligence Surveillance Act (FISA) established oversight rules
  - including special secret FISA court

Example: Trump campaign controversy

- President Trump has accused the NSA of spying on his campaign
- His version: NSA obtained FISA court order through concerns of collusion with Russians

Example: The Snowden documents

- In 2013 Whistleblower Edward Snowden leaked a large collection of documents about massive NSA surveillance programs
- NSA collects data from the servers of Facebook, Google, Microsoft
- phone record **metadata** from Verizon on all American customers
- And other programs

Communication Discussion Questions

- Do you think E-mail should enjoy special protection?
- What about text messages?
- Protection against whom?
  - Government?
  - Hackers?
  - Internet providers?
  - Mail service providers (Google, MS etc)?

Privacy Principles for Government data

The Privacy Act

- Restricts the data in U.S. government records to what is “relevant and necessary” to legal purposes
- Requires federal agencies to publish a notice of their record systems
- Allows people to access their records and correct inaccurate information
- Requires procedures to protect data security
- prohibits disclosure of information about a person without their consent

Exercise

- Consider problem cases like
  - snooping in tax records
  - sale of government information to outsiders (e.g. credit card fraudsters)
  - intercepting communications as revealed by Snowden
- Which principles of the privacy act were violated?

Expectation of Privacy

- What information is protected by privacy laws?
- Answer: when a reasonable person can expect it to be private
- E.g.
  - private conversations
  - locations (tracking, imaging)
- Special Protections
  - medical, financial records
  - personal information of minors

What is not protected?

- Public records (e.g., government salaries, bankruptcies, political donations)
- Business transactions: police do not need warrant
  - but in Switzerland, bank transactions are confidential
  - supports use of transaction data by platforms (e.g. gaming platforms)
- information in public view

Public Viewing

- Video surveillance is legal:
  - > 500,000 Cameras in England.
  - used after Vancouver Stanley cup riots
- It is generally legal to film people without their permission in public but not in private
- Smartphones make it much more likely to be recorded by strangers

The Right to Record

- The Bus Uncle was the most viewed Youtube video in May 2006
- There is special protection for the right to record police officers
- History of recording police abuse
  - Rodney King video

Under construction

International Perspectives

Canadian Privacy Law

- Similar to U.S. law in approach and principles.
- Generally stronger protections:
  - more control over information
  - more enforcement and regulation
  - less access by government agencies
- Two Main Federal Laws:
  - Personal Information Protection and Electronic Documents Act (business)
  - Privacy Act (government)
- Supervised by Privacy Commissioners (federal and provincial)

Bill C-51

- Passed by the Harper government in 2015
- Increases access to information by law enforcement agencies (RCMP, CSIS)
- Hotly debated
- RCMP say encryption is still a problem for them

European Union Law

- Stronger laws than U.S.
- Sending European personal data to U.S. allowed only if U.S. recipient follows strict rules (the Privacy Shield)
- EU data to Canada is okay

EU and the Right to Be Forgotten

- EU Court of Justice: A person can require search engine companies to prevent links to certain kinds of personal information from being shown.
- Should Canada adopt a right to be forgotten?
- What about other data holders, e.g. facebook? What about messages?

Privacy Protection

Technological Solutions: Privacy Protection Tools

- Encryption
- Do Not Track Settings
- Anonymizers/Virtual Private Networks
- Private Web Browsers (e.g. DuckDuckGo)
- cookie/ad disablers
- spyware scanners

Advocacy Groups

- Privacy Rights Clearing House collects tutorials, software, videos
- The Electronic Privacy Information Center is an advocacy group
- The Canadian Public Interest Advocacy Centre addresses many privacy issues
- BC Freedom of Information and Protection of Privacy Association

Key Concepts

Summary

Privacy

- Privacy has three aspects
  - freedom from surveillance
  - control of personal information, especially publication
  - freedom from intrusion
- The Fair Information Principles guide the use of personal information in IT

Privacy Threats

- Surveillance by companies and governments
- Data breaches and Secondary uses lead to loss of control

Legal Concepts for Government Information Use

- Freedom from **Unreasonable Search**: government officials must show probable cause and (often) obtain warrant to collect protected information
- Information is protected when there is a **reasonable expectation of privacy**

Viewpoints on Business Information Use

- Free Market Viewpoint: users **consent** to use of their information in exchange for services and other benefits
- Consumer Protection View:
  - privacy is a right
  - consumers not in a position to negotiate
  - consumers entitled to control over their information, especially secondary uses