RMIT School of Computer Science and IT

Course Notes

COSC1147

Semester 2, 2017

Week 08

Lecture Component

- Privacy in the Electronic Global Metropolis

Privacy and Cybertechnology

- Privacy issues involving cybertechnology affect all of us, regardless of whether we have ever owned or even used a networked computer.
- Consider the amount of personal information about us that can be acquired from our commercial transactions in a bank or in a (physical) store.

Privacy and Cybertechnology (Continued)

- Also, consider that closed circuit television cameras (CCTVs) located in public places and in shopping malls record many of your daily movements as you casually stroll through those environments.
- Current Web-based applications such as Google Street View (a feature of Google Earth and Google Maps) make use of satellite cameras and global positioning system (GPS) software that enable users to zoom in on your house or place of employment and potentially record information about you.
- What about drones around us?

Privacy and Cybertechnology (Continued)

- Even if you use the Internet solely for recreational purposes, your privacy is threatened.
- Personal data, including data about our Web-browsing interests, can now easily be acquired by organizations whose need for this information is not always clear.
- A user's personal data acquired via his/her online activities can be sold to third parties.

Privacy and Cybertechnology (Continued)

- Privacy concerns now affect many aspects of our day-to-day lives – from commerce to healthcare to work.
- So, we have categories such as:
  - consumer privacy,
  - medical/healthcare privacy,
  - employee/workplace privacy.

Government accessing our data

- This was published in The Age: http://www.news.com.au/technology/online/telstra-transparency-report-shows-nearly-85000-customer-data-records-seen-by-police-government/story-fnjwmwrh-1227044095538
- Do you think this is ethical and justified?

Privacy and Cybertechnology (Continued)

- Are any privacy issues unique to cybertechnology?
- Privacy concerns have been exacerbated by cybertechnology in at least four ways, i.e., by the:

1. *amount* of personal information that can now be collected;
2. *speed* at which personal information can now be transferred and exchanged;
3. *duration* of time in which personal information can now be retained;
4. *kind* of personal information (such as transactional information) that can be acquired.

What is Personal Privacy

- Privacy is a concept that is difficult to define.
- We sometimes speak of an individual's privacy as something that can be:
  - lost,
  - diminished,
  - intruded upon,
  - invaded,
  - violated,
  - breached.

What is Privacy (continued)?

- Privacy is sometimes viewed in terms of something that can be *diminished* (i.e., as a repository of personal information that can be eroded gradually) or *lost* altogether.
- Privacy is sometimes also construed in terms of the metaphor of a (spatial) zone that can be *intruded* upon or *invaded*.
- Privacy is also sometimes analyzed in terms of concerns affecting the confidentiality of information, which can be *breached* or *violated*.

Can Privacy Be Preserved in the Digital Era?

- Scott McNealy, CEO of Sun Microsystems, uttered his now famous remark to a group of reporters: *You have zero privacy anyway. Get over it*.
- But some believe that not all has yet been lost in the battle over privacy.
- For example, some privacy advocates staunchly believe that we should be vigilant about retaining and safeguarding what little privacy we may still have.

Is Protecting Personal Privacy Still Considered an Important Goal?

- Can the current privacy debate be better understood in terms of differences that reflect *generational* attitudes?
- For many "Millennials," privacy does not always seem to be of paramount importance.
- Consider, for example, that many Millennials seem eager to share their personal information widely on social networking services such as Facebook.
- But for many older people, including Baby Boomers, privacy is still highly valued.
- Let us see – what we think about this?

Cybertechology-related Techniques that Threaten Privacy

- We examine three techniques that threaten privacy:

1) *data-gathering* techniques used to collect and record personal information, often without the knowledge and consent of users.
2) *data-exchanging* techniques used to transfer and exchange personal data across and between computer databases, typically without the knowledge and consent of users.
3) *data-mining* techniques used to search for patterns implicit in large databases in order to generate consumer profiles based on behavioural patterns discovered in certain groups.

Cybertechnology Techniques Used to Gather Personal Data

- Personal data has been gathered at least since Roman times (census data).
- Roger Clarke uses the term *dataveillance* to capture two techniques made possible by cybertechnology:

a) surveillance (data-monitoring),

b) data-recording.

Internet Cookies as a Surveillance Technique

- “Cookies” are files that Web sites send to and retrieve from the computers of Web users.
- Cookies technology enables Web site owners to collect data about those who access their sites.
- With cookies, information about one’s online browsing preferences can be “captured” whenever a person visits a Web site.

Cookies (Continued)

- The data recorded via cookies is stored on a file placed on the hard drive of the user's computer system.
- The information can then be retrieved from the user's system and resubmitted to a Web site the next time the user accesses that site.
- The exchange of data typically occurs without a user's knowledge and consent.

Can the Use of Cookies be Defended?

- Many proprietors of Web sites that use cookies maintain that they are performing a service for repeat users of their sites by customizing a user's means of information retrieval.
- For example, some point out that, because of cookies, they are able to provide a user with a list of preferences for future visits to that Web site.

Arguments Against Using Cookies

- Some privacy advocates argue that activities involving the monitoring and recording an individual's activities while visiting a Web site violates privacy.
- Some also worry that information gathered about a user via cookies can eventually be acquired by or sold to online advertising agencies.

RFID Technology as a Surveillance Technique

- RFID (Radio Frequency IDentification) consists of a *tag* (microchip) and a *reader*:
- The tag has an *electronic circuit*, which stores data, and *antenna* that broadcasts data by radio waves in response to a signal from a reader.
- The reader contains an *antenna* that receives the radio signal, and *demodulator* that transforms the analogue radio into suitable data for any computer processing that will be done.

RFID Technology (Continued)

- RFID transponders in the form of “smart labels” make it much easier to track inventory and protect goods from theft or imitation.
- RFID technology also poses a significant threat to individual privacy.
- Critics worry about the accumulation of RFID transaction data by RFID owners and how that data will be used in the future.

RFID Technology (Continued)

- Roughly 40 million Americans carry some form of RFID device every day.
- Privacy advocates note that RFID technology has been included in chips embedded in humans, which enables them to be tracked.

RFID Technology (Continued)

- Like Internet cookies (and other online data gathering and surveillance techniques), RFID threatens individual privacy.
- Unlike cookies, which track a user's habits while visiting Web sites, RFID technology can track an individual's location in the off-line world.
- RFID technology also introduces concerns involving "locational privacy" (see Chapter 12).

Cybertechnology and Government Surveillance

- As of 2005, cell phone companies are required by the FCC in USA to install a GPS (Global Positioning System) locator chip in all new cell phones.
- This technology, which assists 911 operators, enables the location of a cell phone user to be tracked within 100 meters.
- Privacy advocates worry that this information can also be used by the government to spy on individuals.

The fierce Australian debate around data retention

- The current government now retains the public metadata.
- The government's mandatory data retention plan, requires Internet Service Providers to save two years of customers' metadata.
- This raises few questions-
  - Is this ethical?
  - Where will this data be stored? What if it is hacked?
  - Who will pay for the ISP's storing this data? – *the naïve customer..*

Computerized *Merging* Techniques

- *Computer merging* is a technique of extracting information from two or more unrelated databases and incorporating it into a composite file.
- Computer merging occurs whenever two or more disparate pieces of information contained in separate databases are combined.

Computer Merging (Continued)

- Imagine a situation in which you voluntarily provide information about yourself to three different organizations – i.e., you give information about your:

1) income and credit history to a lending institution in order to secure a loan;
2) age and medical history to an insurance company to purchase life insurance;
3) views on certain social issues to a political organization you wish to join.

Computer Merging (Continued)

- Each organization has a legitimate need for information to make decisions about you; for example:
- insurance companies have a legitimate need to know about your age and medical history before agreeing to sell you life insurance;
- lending institutions have a legitimate need to know information about your income and credit history before agreeing to lend you money to purchase a house or a car.

Computer Merging (Continued)

- Suppose that information about you in the insurance company's database is merged with information about you in the bank's database or in the political organization's database.
- When you gave certain information about yourself to three different organizations, you authorized each organization to have specific information about you.
- However, it does not follow that you thereby authorized any one organization to have some combination of that information.

Computer *Matching*

- *Computer matching* is a variation of computer merging.

- Matching is a technique that cross-checks information in two or more databases that are typically unrelated to produce "matching records" or "hits."

Computer Matching (Continued)

- In practices involving federal and state government organizations, computerized matching has been used by various agencies and departments to identify:
- *potential* law violators;
- individuals who have *actually* broken the law or who are suspected of having broken the law (welfare cheats, deadbeat parents, etc.).

Computer Matching (Continued)

- Income tax records could be matched against state motor vehicle registration records (looking for individuals reporting low incomes but owning expensive automobiles).
- Consider an analogy in physical space where your mail is matched (and opened) by authorities to catch criminals suspected of communicating with your neighbours.

Computer Matching (Continued)

- Some naïve people always say:

  If you have nothing to hide, you have nothing to worry about.

- Others use the following kind of argument:

  1. Privacy is a legal right.
  2. Legal rights are not absolute.
  3. When one violates the law (i.e., commits a crime), one forfeits one's legal rights.
  4. Therefore, criminals have forfeited their right to privacy.

Data Mining

- Data mining involves the indirect gathering of personal information via an analysis of implicit patterns discoverable in data.
- Data-mining activities can generate new and sometimes non-obvious classifications or categories.
- Individuals whose data is mined could become identified with or linked to certain newly created groups that they might never have imagined to exist.

Data Mining (Continued)

- Current privacy laws offer individuals little-to-no protection for how personal information that is acquired through data-mining activities is subsequently used.
- Yet, important decisions can be made about individuals based on the patterns found in the personal data that has been “mined.”
- Some uses of data-mining technology raise special concerns for personal privacy.

Data Mining (Continued)

- Why is mining personal data controversial?
- Unlike personal data that resides in explicit records in databases, information acquired about persons via data mining is often derived from implicit patterns in the data.
- The patterns can suggest "new" facts, relationships, or associations about that person, such as that person's membership in a newly "discovered" category or group.

Data Mining (Continued)

- Much personal data collected and used in data-mining applications is generally considered to be information that is neither confidential nor intimate.
- So, there is a tendency to presume that personal information generated by or acquired via data mining techniques must by default be *public* data.

Data Mining (Continued)

- Review Scenario 5-6 (in the text) involving Lee, a (hypothetical) 35-year old executive named Lee, who:
  - applies for an car loan for a BMW;
  - has an impeccable credit history.
- A data-mining algorithm "discovers" that:

I. Lee belongs to a group of individuals likely to start their own business;

II. people who start business in this field are also likely to declare bankruptcy within the first three years;

- Lee is denied the loan for the BMW based on the profile revealed by the data-mining algorithms, despite his credit score.

Data Mining (Continued)

- Although the preceding scenario (involving Lee) is merely hypothetical, an actual case (that was similar to this) occurred in 2008.
- In that incident, a person had two credit cards revoked and had the limit on a third credit card reduced because of certain associations that the company made with respect to *where* this person:
  - shopped,
  - lived,
  - did his banking.

Data Mining (Continued)

- In that case, a data-mining algorithm used by the bank “discovered” that this person (whose credit cards were revoked):
- purchased goods at a store where typical patrons who also purchased items there defaulted on their credited card payments;
- lived in an area that had a high rate of home foreclosures, even though he made his mortgage payments on time.

Web Mining: Data Mining on the Web

- Traditionally, most data mining was done in large "data warehouses" (i.e., off-line).
- Data mining is now also used by commercial Web sites to analyze data about Internet users, which can then be sold to third parties.
- This process is sometimes referred to as "Web mining."

Techniques Used to Manipulate Personal Data

Data **Merging**	A data-exchanging process in which personal data from two or more sources is combined to create a "mosaic" of individuals that would not be discernable from the individual pieces of data alone.
Data **Matching**	A technique in which two or more unrelated pieces of personal information are cross-referenced and compared to generate a match or "hit," that suggests a person's connection with two or more groups.
Data **Mining**	A technique for "unearthing" implicit patterns in large databases or "data warehouses," revealing statistical data that associates individuals with non-obvious groups; user profiles can be constructed from these patterns.

Public vs. Non-Public Personal Information

- *Non-Public Personal Information* (or *NPI*) refers to sensitive information such as in one's financial and medical records.
- NPI currently enjoys some legal protection.
- Many privacy analysts are now concerned about a different kind of personal information called *Public Personal Information* (or *PPI*).
- PPI is non-confidential and non-intimate in character, and is generally not legally protected.

Privacy Concerns Affecting PPI

- Why does the collection of PPI by organizations generate privacy concerns?
- Suppose some organization learns that that you are a student at Technical University; you frequently attend university basketball games; and you are actively involved in your university's computer science club.
- In one sense, the information is personal because it is about *you* (as a person);but it is also about what you do in the public sphere.

PPI (Continued)

- Review Scenarios 5-8 and 5-9 (in the textbook), which contrast shopping in a physical store with shopping online.
- But both scenarios reveal problems with regard to protecting *personal privacy in public*, in an era when data mining is typically used in commercial transactions.

Search Engines and Personal Information

- Search engines can be used to:

i. acquire personal information about individuals (as illustrated in the discussion of the Gawker/Stalker site in the text).

ii. reveal to search facilities data about which Web sites you have visited, as illustrated in Scenario 5-10 (in the text), which describes how Google users' search requests were subpoenaed by the U.S. Government.

Accessing Public Records via the Internet

- What are public records, and why do we have them?
- In the past, one had to go to municipal buildings to get public records.
- Review Scenarios 5-11 and 5-12 (in the text), describing online access to two different kinds of public records (at state and local levels).
- Should those records have been made available online to the public?

Can Technology Be Used to Protect Personal Privacy?

- Privacy advocates tend to argue for stronger privacy legislation.
- But groups in the commercial sector tend to oppose strong privacy laws, arguing instead for voluntary industry self-regulation.
- Can *Privacy Enhancing Tools*, or *PETs*, provide an acceptable compromise?

Privacy Enhancing Technologies (PETs)

- PETs are tools that users can employ to protect:
- their personal identity, while navigating the Web;
- the privacy of their communications (such as email) sent over the Internet.

PETs (Continued)

- Two challenges involving PETs with respect to ordinary users include:

1) educating ordinary users about the existence of these tools;
2) preserving the principle of informed consent for users who opt for these tools.

Educating Users About PETs

- How are ordinary users supposed to find about PETs?
- With PETs, the default has been that users must:
  - discover that these tools actually exist;
  - learn how to use them.
- Is this expectation regarding users and PETs a reasonable one?

PETS and the Problem of Informed Consent

- Users can (consent to) enter into an agreement with Web sites that have privacy policies.
- Currently, however, users must typically "opt out" of having data about them collected.
- The default view is that users have opted in, unless they specifically indicate otherwise.
- Also, it is not clear that PETs protect against nonconsensual uses (e.g., secondary and future uses) of one's personal data (as the Toysmart incident, described in the textbook, suggests).

Privacy Legislation and Industry Self-Regulation

- Can industry adequately self-regulate privacy through voluntary controls, instead of strong privacy legislation?
- What kinds of assurances from vendors do online consumers need regarding the protection of their privacy?
- Consider again the incident involving (the now defunct) Toysmart.com (described in the textbook).

Google's 2012 Privacy Policy

- Review Scenario 5-13 in the text for information about Google's comprehensive privacy policy designed to cover its suite of applications.
- One advantage is that the privacy policy is comprehensive; so the same privacy rules apply to anyone using any Google application.
- Another advantage is that Google's privacy policy is explicit and transparent.
- However, this policy has also been very controversial and it has been criticized by some privacy advocates.

Critics of Google's Privacy Policy Worry Because in Their View

- It is not clear how Google will use all of the personal information that it can now access so easily.
- No one outside Google fully understands how the search engine company uses that information to manipulate (i.e., tailor or personalize) the search results a user receives for his or her search queries.
- Additionally, it is not clear whether one's personal information collected from the various Google services will be used only internally, or will also be available to advertisers and information merchants outside the company.

Google's Privacy Critics (Continued)

- Some critics worry whether users can trust Google – a company that officially embraces the motto: "do not be evil" – to abide by its new privacy policy.
- For example, many people who used Apple's Safari Web browser on their computers and iPhones were under the impression that Google was not able to track their browsing activities.
- However, it was discovered Google had used software code that tricked the Safari browser, thus enabling Google to track the activities of those using that browser.

Google's Privacy Critics (Continued)

- Google responded to its critics by disabling the controversial software code shortly after the incident was reported in *The Wall Street Journal*.
- Safari users were informed by Google that they could rely on Safari's privacy settings to prevent tracking by Google in the future.
- But some critics have remained sceptical.
- Because of concerns involving distrust of Google and other commercial Web sites to regulate themselves, privacy advocates believe that explicit privacy laws are needed to protect users.

Drones in Australia

- Australian privacy law needs to be updated to take into account potential breaches of privacy by remotely piloted aircraft, a report by the House of Representatives Standing Committee on Social Policy and Legal Affairs has recommended.
- The committee, chaired by Nationals MP George Christensen, investigated the impact that drones are having in Australia, and offered a number of recommendations in its report (PDF) for how the technology should be treated under law in order to protect privacy.
- Drones in Austalia: [http://www.youtube.com/watch?v=SPLHlL5gLZw]

Drones in Australia

- The report stated that while remotely piloted aircraft can offer economic benefits and safety improvements, there were a number of incidents reported that raise questions about the safety of drones, and the potential privacy intrusions associated with the use of drones.
- *What do you think?*
- http://www.zdnet.com/au/mps-decide-drones-invade-australian-privacy-7000031534/

Drone Laws in Australia

- Hobbyist/non-commercial flights
- Very small (under 2 kg)
- Commercial
- Large, small, micro (weight classifications)
- Unmanned free balloons, fireworks, rockets …
- https://www.rpastraining.com.au/casr-101-uav-drone-legal-or-illegal

Suggested Reading

- Textbook: Chapter 5, Privacy in Cyberspace, *Pages 131-146, 162-166*
- Data gathering in Australia [http://www.youtube.com/watch?v=KeVq2QEUBTM]
- RFID [http://www.youtube.com/watch?v=MAA9JpGraoU]
- Privacy law in Australia [http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform]
- Social media experiment [http://www.youtube.com/watch?v=5P_0s1TYpJU]
- Scary Privacy prank [http://www.youtube.com/watch?v=YLWmjpPoJHk