ILLINOIS TECH | College of Computing

ITMM 485 / 585
Dr. Gurram Gopal

Legal and Ethical Issues in Information Technology

1

ILLINOIS TECH | College of Computing

Ch5: PRIVACY AND CYBERSPACE
P2: What is Value of Privacy? How does Cybertechnology and Data Warehousing and Mining impact Privacy?

2

Chapter Learning Objectives:

Upon completion of this lesson the students should be able to:

- Describe and discuss privacy issues driven by data merging, matching and mining
- Explain privacy concerns arising from use of search engines, social media, and online public records
- Describe and discuss the use of Privacy Enhancement Tools
- Recall U.S. and European Union privacy laws and describe their application and use

3

Module Learning Objectives:

Upon completion of this lesson the students should be able to:

- Explain and Discuss what kind of value is privacy
- Elaborate on Cybertechnology tools used to gather and mine data

4

Can Privacy Be Preserved in the Digital Era?

- **Scott McNealy, a former CEO of Sun Microsystems, proclaimed his now famous remark to a group of reporters: *You have zero privacy anyway. Get over it*.**
- **Others authors have expressed concerns about the "death of privacy."**
- **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.**

5

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," who are now college-aged, 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 Americans, including Baby Boomers, privacy is still highly valued.**
- **So the relative importance of privacy may vary considerably among the generations, at least in the U.S.**

6

What Kind of Value is Privacy?

- Three distinct questions can be distinguished with respect to privacy as a *value*:

1. Is privacy an *intrinsic* value, or is it an *instrumental* value?
2. Is privacy *universally* valued, or is it valued mainly in Western industrialized societies (where greater importance is placed on the individual than on the broader community?)
3. Is privacy an important *social* value (as well as an individual value)?

7

Is Privacy an Intrinsic Value or an Instrumental Value?

- Is privacy something that is valued for its own sake?
- In other words, is it an *intrinsic value*?
- Or, is privacy valued as a means to some further end?
- Is it merely an *instrumental value*?

8

Is Privacy an Intrinsic or an Instrumental Value (Continued)?

- Privacy does not seem to be valued for its own sake, and thus does not appear to have intrinsic worth.
- But Charles Fried (1990) privacy also seems to be more than merely an in- strumental value because it is *necessary* (rather than merely *contingent*) for achieving important human ends.

9

Is Privacy an Intrinsic or an Instrumental Value (Continued)?

- Fried notes that privacy is necessary for important human ends such as *trust* and *friendship*.
- Moor believes that privacy can be viewed as an expression of a "core value" – viz., *security*, which is essential for "human flourishing."

10

Privacy as a Universal Value

- Privacy has at least some importance in all societies, but it is not valued the same in all cultures.
- For example, privacy tends to be less valued in many non-Western nations, as well as in many rural societies in Western nations.
- Privacy also tends to be less valued in some democratic societies where national security and safety are considered more important than individual privacy (e.g., as in Israel).

11

Privacy as an Important Social Value

- Priscilla Regan notes that we tend to underestimate the importance of privacy as an important *social value* (as well as an individual value).
- Regan also believes that if we frame the privacy debate in terms of privacy as a social value (essential for democracy), as opposed to an individual good, the importance of privacy is better understood.

12

Cybertechology-related Techniques that Threaten Privacy

- We examine two distinct cyber-related 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 analysis* techniques, including data mining, used to manipulate large data sets of personal information to discover patterns and generate consumer profiles (also typically without the knowledge and consent of users).

13

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.

14

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.

15

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.

16

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.

17

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.

18

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 analog radio into suitable data for any computer processing that will be done (Lockton and Rosenberg, 2005).

19

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.
- Privacy advocates note that RFID technology has been included in chips embedded in humans, which enables them to be tracked.

20

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).

21

Cybertechnology and Government Surveillance

- As of 2005, cell phone companies are required by the FCC 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.

22

Analyzing Personal Data: Big Data, Data Mining, and Web Mining

- What, exactly, is *Big Data*?
- John Stuart Ward and Adam Barker (2013) note that while the term "big data" has become "ubiquitous," it also has no precise or "unified single" meaning.
- They also point out that the definitions of big data put forth thus far are not only "diverse," but are often "contradictory" as well.

23

Big Data

- Initially, one might assume that the concept of *big data* simply refers to the size or scale of the data being analyzed.
- For example, Danah Boyd and Kate Crawford (2012) suggest that big data can be understood mainly in terms of its "capacity to search, aggregate and cross-reference *large data sets*."

24

Big Data (Continued)

- Definitions of big data that focus on capturing the large size of the data sets involved often view big data primarily in terms of its ***volume***.
- Other definitions include factors affecting the "three V's":
  - *variety*,
  - *velocity*,
  - *veracity*.
- Whereas "velocity" captures the speed ("fast data in/out") involved in the process, "veracity, refers to the notion of trust in the (big) data analysis that needs to be established for business decision making.

25

Big Data (Continued)

- The concept of big data is a far more complex phenomenon than merely the size, or volume, of the data involved.
- As Deborah Poskanzer (2015) points out, in the case of big data, "more isn't just more—more is different."
- She further suggests that big data can be better understood as a "new mode of knowledge production."

26

Big Data (Continued)

- Regardless of which expression we use to describe this phenomenon – big data, data mining, or KDD – serious privacy concerns have been generated by it.
- Some believe that these kinds of concerns justify the need for a new legal category of privacy, which some call "group privacy."
- Many, if not most, of the kinds of privacy concerns currently associated with big data had already been introduced by the use of various ***data mining*** techniques, beginning in the 1990s.

27

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.

28

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.

29

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.

30

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.

31

Data Mining (Continued)

- Review Scenario 5-5 (in the text) involving Jane, a (hypothetical) real estate professional, who:
- applies for a mortgage at XYZ Credit Union;
- has an impeccable credit history.
- A data-mining algorithm "discovers" that:

I. Jane 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;

- Jane is denied the mortgage loan based on the profile revealed by the data-mining algorithms, despite his credit score.

32

Data Mining (Continued)

- Although the preceding scenario (involving Jane) 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 (Stuckey 2009).

33

Data Mining (Continued)

- In that (2008) 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.

34

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."
- Examine the "Facebook Beacon" incident (in the textbook) as an example of Web mining.

35

36