


**ILLINOIS TECH** | College of Computing

**ITMM 485 / 585**  
**Dr. Gurram Gopal**

Legal and Ethical Issues in  
 Information Technology



1

Ethical Concepts and Theories

**ILLINOIS TECH** | College of Computing

**Ch5: PRIVACY AND CYBERSPACE**  
**P3: Non-Public and Public**  
**Personal Information; PETs;**  
**Self Regulation**



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

ITMM 485/585: Legal and Ethical Issues in IT Slide 1-3

3

**Module Learning Objectives:**

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

- Explain the difference between NPI and PPI
- Discuss and apply common Privacy Enhancing Technologies (PETs) including
- Articulate limitations of Self-Regulatory Controls (PETs and Trust Seals)

ITMM 485/585: Legal and Ethical Issues in IT Slide 1-4

4

**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.

5

**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.

6

## PPI (Continued)

- In the past, it was assumed that there was no need to protect the kind of information we now call PPI, because it was viewed as simply public information.
- Nissenbaum (2004b) believes that our assumptions about not needing to protect PPI are no longer tenable because of what she views as a misleading assumption:

*There is a realm of public information about persons to which no privacy norms apply.*

7

## PPI (Continued)

- Review Scenarios 5-6 and 5-7 (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.

8

## Search Engines and Personal Information

- Search engines can be used to:
  - acquire personal information about individuals (as illustrated in the discussion of the Gawker/Stalker site in the text).
  - reveal to search facilities data about which Web sites you have visited, as illustrated in the controversial incident in which describes how Google users' search requests were subpoenaed by the U.S. Government.

9

## Privacy Legislation and Industry Self-Regulation

- 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?

10

## Privacy Enhancing Technologies (PETs)

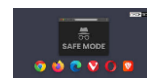
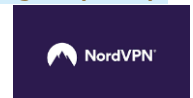
- PETs are tools that users can employ to protect:
  - their personal identity, while navigating the Web;
  - the privacy of their communications (such as email) sent over the Internet.
- Other kinds of PETs, e.g., used in e-commerce contexts, include "trust marks/ seals" such as TRUSTe.

11

## Privacy Enhancing Technologies (PETs)

### Key methods used by PETs

- ❖ Encryption
- ❖ Data Masking
  - Anonymization
  - Obfuscation
- ❖ Differential Privacy
- ❖ Advanced Metadata Applications



12

## Challenges with PETs

- How are ordinary users supposed to find about PETs and learn how to use them?

## Informed Consent

- What is the default? opt-in or opt-out

ITMM 485/585: Legal and Ethical Issues in IT

Slide 9-23

13

## Limitations of Self-Regulatory Controls (PETs and Trust Seals)

- Are industry self-regulation practices (such as TRUSTe) and technology-based controls (e.g., PETs) adequate?
- 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).

14

## Does Google's 2012 Privacy Policy Help Resolve Users' Worries?

- Review Google's comprehensive privacy policy designed to cover its suite of applications (as described in the textbook).
- 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.

15

## Google's Privacy Policy (Continued)

- Critics of Google's privacy policy believe that we should be concerned because:
- 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.

16

## 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.

17

## Google's Privacy Critics (Continued)

- Google has 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 (Anguin and Valentino-DeVries, 2102).
- But some critics have remained skeptical.
- 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.

18

