

ITMM 485 / 585
Dr. Gurram Gopal**Legal and Ethical Issues in
Information Technology**

1

Ch5: PRIVACY AND CYBERSPACE
P4: U.S. and European Union
privacy laws and data protection

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

Privacy Laws and Data Protection

- Privacy laws and data-protection principles in Europe and the U.S. include the:
- European Union (EU) 1995 Privacy Directive;
- U.S. Privacy Act of 1974, and HIPAA (Health Insurance Portability and Accountability Act).

4

The EU Privacy Directive

- EU nations, through the implementation of strict "data protection" principles, have been far more aggressive than the United States in both anticipating and addressing privacy concerns raised by cybertechnology.
- The European community synthesized the "data protection" laws of the individual European nations into the (comprehensive) EU Directive 95/46/EC of the European Parliament and of the Council of Europe of 24 October 1995.
- This framework is commonly referred to as the EU Directive on Data Protection (or "Privacy Directive").
- The EU Privacy Directive was designed to protect the individual rights of citizens and control data processing within the EU, while also facilitating the free flow of data.

5

6



EU Privacy Directive (Continued)

- Among the Principles comprising the EU Privacy Directive are two worth noting (for our purposes):
- Data Quality
- Transparency.
- The Data Quality Principle is concerned with protecting the data subject's reasonable expectations concerning the processing of data about that subject (ensuring that the personal data being processed is true, updated, and properly kept).
- The Transparency Principle grants the data subject the rights to be informed, to contest, to correct, and "to seek judicial redress."

7



EU Privacy Directive (Continued)

- The EU nations have also set up privacy oversight agencies with privacy protection commissions and boards in the various European nations.
- Each member state of the EU is required to have a Data Protection Authority (DPA).
- DPAs are empowered to check to see that all of the laws are being followed in the processing of personal data, and they can impose very severe sanctions when personal data is processed illegally.
- In Europe, willful data-protection breaches may also be criminal offenses, and can even rise to the level of felonies in certain circumstances.

8



EU Privacy Directive (Continued)

- A relatively recent challenge for the EU Privacy Directive whether users should have a right to have certain kinds of personal information about them deleted, or at least "delinked" from search-engine indexes.
- This "right" is controversial because it:
- has international implications, given the flow of information across the porous boundaries of cyberspace.
- applies to online personal information that is shown to be either inaccurate or no longer "relevant."

9



A Right to "Be Forgotten" or to "Erasure"

- Examine Scenario 5-8 in the textbook, involving "Philip Clark."
- Should Philip have the right to have the link to the 20-year-old (online version of the) newspaper story about his "underage drinking" arrest removed from the list of returns from Google searches under his name?
- Does Philip also have the right to have the online content about this story deleted or digitally "erased" as well?
- Is this particular information about Philip still "relevant"?
- These questions are at the heart of a controversial new EU privacy law – namely, *The Right to Be Forgotten*.

10



The Right to Be Forgotten (RTBF)

- Review the actual case of Mario Costeja González, described in the text, involving RTBF.
- The Spanish court agreed with González.
- Should that decision hold in other EU countries as well?
- Google challenged the González decision, appealing to the European Court of Justice (ECJ).
- The ECJ eventually ruled in favor of González.
- But several arguments have been (and continue to be) put forth on both sides of the RTBF debate.

11



Arguments Opposing RTBF

- Major search engine companies and journalists/publishers have been among RTBF's staunchest opponents.
- Search engine companies generally make two different kinds of claims, arguing that they:
 - 1) do not control content and on the Internet (and thus cannot be held responsible for the relevance, or accuracy, of the content on sites to which they provide links);
 - 2) cannot be expected to respond to all of the links requested by users (even if the information being linked to is either inaccurate or no longer relevant, because doing so would be too *impractical*, if not impossible).

12

Arguments Opposing RTBF (continued)

- As already noted, journalists and publishers have also opposed RTBF.
- They believe that being required to comply with RTBF is:
 - a) tantamount to “Internet censorship” (because it violates “freedom of expression”);
 - b) harmful to the general public (because it interferes with a citizen’s “right to know”).

13

Establishing “Appropriate” Criteria for RTBF

- While the European Court of Justice ruled in favor of RTBF (May 2014), it did not provide precise criteria for search engine companies to comply with the new privacy principle.
- Google has since established an advisory council to come up with appropriate criteria.
- Arguably, two important factors need to be taken into consideration:
 1. the nature of the *personal information* itself;
 2. the *context(s)* in which this information flows.

15

Privacy in the U.S.

- Not a Constitutional right but has been construed by the courts : “Reasonable expectation” of privacy
 - ❖ right not to be disturbed
 - ❖ right to be anonymous
 - ❖ right not to be monitored
 - ❖ right not to have one’s identifying information exploited

17

Arguments Defending RTBF

- Arguments supporting RTBF generally fall into two broad categories.
- Supporters claim that this privacy principle is needed to:
 - 1) Prevent innocent people from being harmed;
 - 2) Protect people whose personal identity evolves over time.

14

EU General Data Protection Regulation

The update to the Privacy Directive, (EU) 2016/679 aka GDPR, affects global organizations that hold or process personal data of any European Union resident

- GDPR definition of “personal data” broader than in current US compliance regulations
- Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy
- Penalties for non-compliance 20 million Euros or 4% of global revenue, whichever is higher

16

U.S. Privacy Laws

- Federal Privacy Act of 1974
- Electronic Communications Privacy Act (ECPA) : 4th Amendment of the U.S. Constitution- Prohibits search & seizure without a warrant
- HIPAA
 - Consumer control of medical information
 - Boundaries on the use of medical information
 - Accountability for the privacy of private information
 - Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
 - Security of health information

18

California Privacy Rights Act

- Creates the California Privacy Protection Agency
- Creates new class of PI –sensitive personal information (SPI)
- Has additional disclosure, opt-out, and use requirements
- All businesses that share personal data are covered but reduces impact on small businesses
- Requires business privacy policies to include information on consumers' privacy rights and how to exercise them
 - the Right to Know - the Right to Opt-Out of Sale
 - the Right to Delete - the Right to Non-Discrimination

ITMM 485/585: Legal and Ethical Issues in IT

Slide 1-19

19

Illinois Protecting Household Privacy Act (PHPA)

- 2022 law prohibits Illinois law enforcement agencies from obtaining household electronic data or directing private third parties to acquire household electronic data without a warrant except where consented to or in specific emergency situations
- Collection of Ring doorbell data requires a warrant

ITMM 485/585: Legal and Ethical Issues in IT

Slide 1-20

20

Illinois Biometric Information Privacy Act (BIPA)

- **Requires entities that use and store biometric identifiers to comply with certain requirements, including consent**
 - ❖ Provides private right of action to recover statutory damages when they do not; no proof of actual damage is required
 - ❖ In the class action suit Patel v. Facebook, Inc., Facebook agreed to a \$650 million settlement for violating this act by using facial recognition to attach names to faces on Facebook without consent of those identified

ITMM 485/585: Legal and Ethical Issues in IT

Slide 1-21

21



ITMM 485/585: Legal and Ethical Issues in IT

Slide 1-22

22