A GIFT OF FIRE

Social, Legal, and Ethical Issues for Computing Technology

Fifth Edition

Chapter 2: Privacy

SARA BAASE

TIMOTHY M. HENRY

Based on slides prepared by Cyndi Chie, Sarah Frye and Sharon Gray.
Fifth edition updated by Timothy Henry

Pearson

1

What We Will Cover

- Privacy Risks and Principles
- New Technologies
- Government Systems

2

Privacy Risks and Principles

Key Aspects of Privacy:

- Freedom from intrusion (being left alone).
- Control of information about oneself.
- Freedom from surveillance (from being tracked, followed, watched).

3

Privacy Risks and Principles

Privacy threats come in several categories:

- Intentional, institutional uses of personal information.
- Unauthorized use or release by "insiders".
- Theft of information.
- Inadvertent (unintentional) leakage of information.
- Our own actions.

4

Privacy Risks and Principles

New Technology, New Risks:

- Government and private databases.
- Sophisticated tools for surveillance and data analysis.
- Vulnerability (weakness) of data.

5

Privacy Risks and Principles

New Technology, New Risks – Examples:

Search query data

- Search engines collect many terabytes of data daily.
- Data is analyzed to target advertising and develop new services.
- Who gets to see this data? Why should we care?

6

Privacy Risks and Principles

New Technology, New Risks – Examples:

<u>Smartphones</u>

- Location apps.
- Data sometimes stored and sent without user's knowledge.

Pearson

7

Privacy Risks and Principles

New Technology, New Risks – Summary of Risks:

- Anything we do in cyberspace is recorded.
- Huge amounts of data are stored.
- People are not aware of collection of data.
- Software is complex.
- Leaks happen.

Pearson

8

Privacy Risks and Principles

New Technology, New Risks – Summary of Risks (cont.):

- A collection of small items can provide a detailed picture.
- Re-identification has become much easier due to the quantity of information and power of data search and analysis tools.
- If information is on a public Web site, it is available to everyone.

9

Privacy Risks and Principles

New Technology, New Risks – Summary of Risks (cont.):

- Information on the Internet seems to last forever.
- Data collected for one purpose will find other uses.
- Government can request sensitive personal data held by businesses or organizations.
- We cannot directly protect information about ourselves. We depend upon businesses and organizations to protect it.

10

Privacy Risks and Principles

Terminology:

- *Personal information* – any information relating to an individual person.

- *Informed consent* – users being aware of what information is collected and how it is used.

- *Invisible information gathering* - collection of personal information about a user without the user's knowledge.

11

Privacy Risks and Principles

Terminology:

- *Cookies* – Files a Web site stores on a visitor's computer.

- *Secondary use* – Use of personal information for a purpose other than the purpose for which it was provided.

- *Data mining* – Searching and analyzing masses of data to find patterns and develop new information or knowledge.

12

Privacy Risks and Principles

Terminology:

- *Computer matching* – Combining and comparing information from different databases (using social security number, for example) to match records.

- *Computer profiling* – Analyzing data to determine characteristics of people most likely to engage in a certain behavior.

13

Privacy Risks and Principles

Two common forms for providing informed consent (permission) are *opt out* and *opt in*:

- *opt out* – Person must request (usually by checking a box) that an organization *not* use information.

- *opt in* – The collector of the information may use information only if person explicitly permits use (usually by checking a box).

14

Privacy Risks and Principles

Discussion Questions:

- *Have you seen opt in and opt out choices? Where? How were they worded?*

- *Were any of them deceptive (misleading)?*

- *What are some common elements of privacy policies you have read?*

15

Privacy Risks and Principles

Fair information principles:

1. Inform people when you collect information.
2. Collect only the data needed.
3. Offer a way for people to opt out.
4. Keep data only as long as needed.
5. Maintain accuracy of data.
6. Protect security of data.
7. Develop policies for responding to law enforcement requests for data.

16

New Technologies

- **Two key problems arise from new technologies:**
  - Much of our personal information is no longer safe in our homes; it resides in huge databases outside our control.
  - New technologies allow the government to search our homes without entering them and search our persons from a distance without our knowledge.

17

New Technologies

- Make possible "noninvasive but deeply revealing" searches.
  - **Particle sniffers, imaging systems, location trackers.**
- What restrictions should we place on their use?
- When should we permit government agencies to use them without a search warrant?

18

Video Surveillance and Face Recognition

- **Security cameras:**
  - Increased security.
  - Decreased privacy.

Pearson

19

Social Networks

- **What *we* do:**
  - Post opinions, gossip, pictures, "away from home" status.
- **What *they* do:**
  - New services with unexpected privacy settings.

Pearson

20

Our Social and Personal Activity

Discussion Questions:

- *Is there information that you have posted to the Web that you later removed? Why did you remove it? Were there consequences to posting the information?*

- *Have you seen information that others have posted about themselves that you would not reveal about yourself?*

21

Life In the Clouds

- Security of online data.
- Convenience.

22

Location Tracking

- Global Positioning Systems (GPS) – Computer or communication services that know exactly where a person is at a particular time.

- Cell phones and other devices are used for location tracking.

- Pros and cons.

23

Government Systems

Databases:

- Data mining and computer matching to fight terrorism.

24

Government Systems

Public Records: Access vs. Privacy

- Public Records – records available to general public (bankruptcy, property, and arrest records, salaries of government employees, etc.).

- Identity theft can arise when public records are accessed.

- How should we control access to sensitive public records?

25

Government Systems

Discussion Questions:

- *What data does the government have about you?*

- *Who has access to the data?*

- *How is your data protected?*

26

National ID Systems

- **Social Security Numbers:**
  - Too widely used.
  - Easy to falsify (alter).

Pearson

27