BIRZEIT UNIVERSITY

Introduction to privacy

COMPUTER SCIENCE DEPARTMENT

COMP438

Dr. Abdallah Karakra

Tuesday, October 22, 2024

What is privacy?

“Being alone.”

What is privacy?

"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"

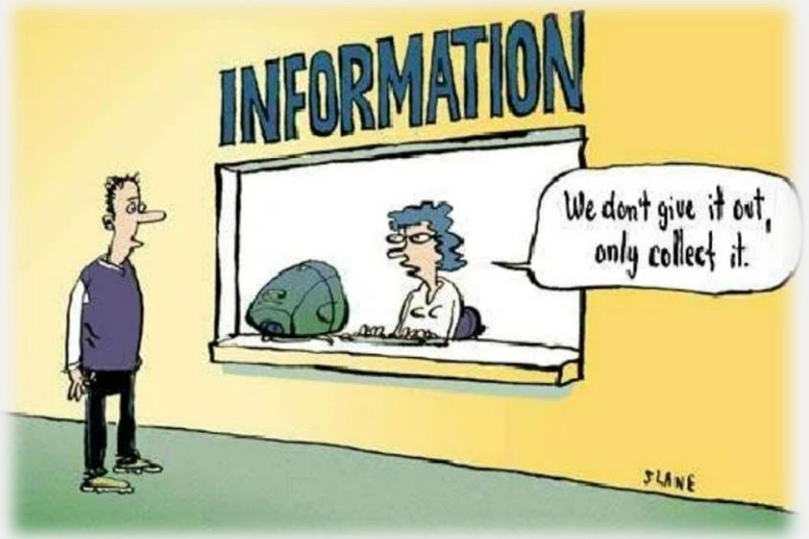
Westin "Privacy and Freedom" 1967

Informational self-determination

Control cover

- Who gets to see it
- Who gets to use it
- What they can use it for
- Who they can give it to
- etc

In a healthcare setting, **informational self-determination** means that patients have control over who accesses their medical records, who is allowed to use their health data, the specific purposes for which their information can be utilized (such as treatment planning), and whether their data can be shared with other healthcare providers.



Westin's four states of privacy

- Solitude
  - individual separated from the group and freed from the observation of other persons

- Intimacy
  - individual is part of a small unit

- Anonymity
  - individual in public but still seeks and finds freedom from identification and surveillance

- Reserve
  - the creation of a psychological barrier against unwanted intrusion - holding back communication

Laws and regulations

- Privacy laws and regulations vary widely throughout the world
- US has mostly sector-specific laws
- European Data Protection Directive requires all European Union countries to adopt similar comprehensive privacy laws

Laws and regulations

- Bank Secrecy Act, 1970
- Fair Credit Reporting Act, 1971
- Privacy Act, 1974
- Right to Financial Privacy Act, 1978
- Cable TV Privacy Act, 1984
- Video Privacy Protection Act, 1988
- Family Educational Right to Privacy Act, 1993
- Electronic Communications Privacy Act, 1994
- Freedom of Information Act, 1966, 1991, 1996

US law

- HIPAA (Health Insurance Portability and Accountability Act, 1996)
  - When implemented, will protect medical records and other individually identifiable health information
- COPPA (Children‘s Online Privacy Protection Act, 1998)
  - Web sites that target children must obtain parental consent before collecting personal information from children under the age of 13
- GLB (Gramm-Leach-Bliley-Act, 1999)
  - The purpose of the GLB Act is to ensure that financial institutions and their affiliates safeguard the confidentiality of personally identifiable information gathered from customer records in paper, electronic or other forms.
  - Requires privacy policy disclosure and opt-out mechanisms from financial service institutions

In short: Privacy policies

- Policies let consumers know about site's privacy practices
- Consumers can then decide whether or not practices are acceptable, when to opt-in or opt-out, and who to do business with
- The presence of privacy policies increases consumer trust

Privacy policy problems

policies are often :

- difficult to understand
- hard to find
- take a long time to read
- change without notice

Privacy policy components

- Identification of site, scope, contact info
- Types of information collected
  - Including information about cookies
- How information is used
- Conditions under which information might be shared
- Information about opt-in/opt-out
- Information about data retention policies
- Information about seal programs
- Security assurances
- Children's privacy

There is lots of information to convey -- but policy should be brief and easy-to-read too!

What is opt-in? What is opt-out?

References

- Prof. Lorrie Cranor's lecture notes
- Stallings & Brown's PowerPoint slides