Bachelor of Engineering in Information Technology

ITM301 Professional Practices in IT

Unit IV: Privacy

Mr. Yeshi Jamtsho
Lecturer

Overview

- Concept Evolution
- Rights to Privacy
- Privacy and Techniques
- US Privacy Laws

Activity

- Name of the Activity: Oversharing Game
- Instructions:
  - Indentify 4 oversharers from the class
  - Provide them the prompt
  - Let them share based on the prompt
  - Reflect Against each oversharer – connecting the dots
- Serious reflection
  - *How much did you reveal without realizing?*
  - *How easy was it for others to piece together your "private" life?*
  - *What could hackers/companies do with this info?*

Foundational Questions

- What does the word “privacy” mean to you?
- Do you think you have privacy when you’re online? Why or why not?
- What kind of information about yourself would you never want to share publicly?
- If you had nothing to hide, would you still care about privacy? Why?
- Who do you trust more with your personal information: your best friend, your parents, your government, or a big tech company? Why?

Foundational Questions Cont..

- When you install an app and it asks for permissions (location, microphone, contacts), do you usually read them carefully or just click “Allow”?
- How would you feel if a stranger read all your WhatsApp messages? What about your browsing history?
- Do you think privacy is a *right* or just a *personal choice*?
- What are some ways you already protect your personal information (online or offline)?
- Is privacy the same as secrecy? Why or why not?

Privacy

- The original privacy concept is *physical privacy*
  - Freedom from intrusion
    - "to be let alone".

- Protecting **privacy** means preventing intruders from entering private properties without authorization.

- Article 7(19) of our Constitution:
  - "*A person shall not be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence nor to unlawful attacks on the person's honour and reputation*".

Privacy Concept Evolution

- With the technology advances, comes the need to extend the privacy concept:
- Freedom from surveillance (from being followed, tracked, watched …)
- The issue first came up when telephone was invented in late 19th century
    - Wire-tapping violates peoples' privacy, even though their physical private properties are not compromised.

Key Aspects of Privacy

- Freedom from intrusion—being left alone
- Control of information about oneself
- Freedom from surveillance (from being followed, tracked, watched, and eavesdropped upon)

Privacy Risks and Principles

Privacy threats come in several categories:

1. Intentional & institutional uses of personal information
2. Unauthorized use or release by “insiders”
3. Theft of information
4. Inadvertent leakage of information
5. Our own actions

Terminology and Principles

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

Terminology and Principles Cont..

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

Terminology and Principles cont…

- Providing informed consent:
  - Opt out – Person must request (usually by checking a box) that an organization not use information
  - Opt in – The collector of the information mat use information only if person explicitlt permits use (usually checking a box)
- How were some opt in and opt out choices you have seen worded (clearly or deceptively)?
- What are some common elements of privacy policies you have read?

Privacy principles for Personal Information

1. Inform people when you collect information about them, what you collect, and how you use it.

2. Collect only the data needed.

3. Offer a way for people to opt out from mailing lists, advertising, and other secondary uses. Offer a way for people to opt out from features and services that expose personal information.

4. Keep data only as long as needed.

5. Maintain accuracy of data. Where appropriate and reasonable, provide a way for people to access and correct data stored about them.

6. Protect security of data (from theft and from accidental leaks). Provide stronger protection for sensitive data.

7. Develop policies for responding to law enforcement requests for data.

Rights to Privacy

How much privacy are we entitled to?

- Privacy is a ***natural right***.(Warren&Brandeis [1890])

Question:

Can we afford absolute privacy right to everyone?

Harms of Too Much Privacy:

- Harder for others to really know a person
- Easier for some people to plan and carry out illegal or immoral activities
- Conflicting with other people’s rights

Rights to Privacy Cont…

- How much privacy are we entitled to?

- Privacy is a *prudential right*. (Benn and Reiman [1984])
  - *Granting privacy rights benefits the society:*
    - Allow people to be unique individuals
    - Foster creativity, spirituality, relationships, etc.
  - *However, privacy rights must be balanced with other rights*

How to Balance?

- Privacy *vs.* Safety and Security
  - E.g. government surveillance
- Privacy *vs.* Desire for Free Expression
  - E.g. news articles
- Privacy *vs.* Convenience
  - E.g. telephone number listing
- Privacy *vs.* Need for Credentials
  - E.g. loan applications

Privacy and Technology

- Technologies have made information collection, storing, and access much easier.
  - Personal info easily become public
  - Databases everywhere
  - Data mining becoming more powerful
  - Surveillance technology becoming more sophisticated
- On the positive side,
  - Encryption techniques

Challenges

- **Footprints and Fingerprints everywhere**
  - Big brother is watching
    - Government surveillance and data mining
  - Big sister is watching
    - Commercial companies have lots of information about you
  - Little brother is watching
    - Public documents become very public
    - Everyone can be a detective

Loss of Privacy

- We are leaving an “electronic trail”
- History of government abuses
- Identity theft
- Loss of privacy = loss of self ???
- Privacy for spiritual growth, creativity

Digital Footprints

- Bank and credit card activities
- Web surfing records
- GPS and cellphones
- Black boxes in cars
- Smart parking garages
- Meta data in documents
- Tracing paper

Public Information

- Personal info can easily become public:
  - Personal info in blogs and online profiles
  - Pictures of ourselves and our families
  - Consumer product registrations

- *Question:*
- Young people seem to put less value on privacy than previous generations.
  - ➢ Is privacy old-fashioned? OR
  - ➢ they don’t understand the risks?

Public Records

- Many records are available to the general public:
  - Property records, bankruptcy records
  - Salaries of government employees
  - Arrest records, etc.

- *Access vs. Privacy:*
  - How should we control access to sensitive public records?

Digital Cameras

- Taking pictures on public property. Does it violate privacy?
    - Google Street View
        - Captures whatever camera sees at the time
    - Digital Cameras in general
        - Panavision 300x optical zoom (see YouTube video for effects)
- ***Laws:***
    - On public property, “if you can see it, you can shoot it” (*additional restrictions on zooming in on people*)
    - You may not be able to publish what you shot

Video Surveillance

- **Examples:**

- The UK has **one surveillance camera for every 12 citizen**.
  - In London, an average person is photographed hundreds of times a day by surveillance cameras

- Mass surveillance in China - close to **200 million surveillance cameras**

Other Technologies

- **Cell phones**: Location Tracking
- **RFID** tags (radio freq. ID)
  - Put into products for inventory control
    - They are never deactivated
  - In passports
    - Terrorists scan cafes/targets for foreigners!
  - Implanted in pets… or people.
- **Cookies** – to track web usage

Government Databases

- In USA, the government maintains many databases.

Among them:

- Census Records,
- FBI NCIC Database

- ***Questions***:
  - Who can create and keep databases of personal information?
  - Who has right to access these databases?

Kinds of Information

- Public Records (Governemnt records)
  - Marriage certificates, arrest records, legal deeds, etc.
- Public Information
  - Info available from companies, Internet, …
- Personal Information
  - What's left? Your secrets?

Code of Fair Information Practices

- Proposed by an US study group in the early 70s.
- Adopted later by many governments, including US:
  - ✓ No secret databases
  - ✓ People should have access to personal information in databases
  - ✓ Organizations cannot change how information is used without consent
  - ✓ People should be able to correct or amend records
  - ✓ Database owners and users are responsible for reliability of data and preventing misuse

Privacy Act of 1974

Codification of the proposed principles.

- Existence of personal-info databases must be disclosed.
- Everyone has a right to know what info about him/her-self is in the databases.
- Consent is required if personal-info is targeted for non-intended uses.

Loopholes of the Privacy Act

- *Only applies to government databases.*
  - Far more info is held in private databases
- *Only covers records indexed by a personal ID.*
  - One has no right to access his/her info if record is not keyed to his/her ID
- *No one is in charge of enforcing the law.*
  - Many exceptions have been given
- *Allows records to be shared among agencies as long as they are for "routine use".*
  - Each agency defines "routine use" for itself

Other US Privacy Laws

- *Family Education Rights and Privacy Act [1974]*
  - Rights to access/change/release educational records are given to student (18yrs or older) or his/ her parents
- *Video Privacy Protection Act [1988]*
  - Videotape service providers cannot disclose rental records without consumer’s written consent

Data Mining

- Info about customers is a valuable commodity
- Searching for patterns or relationships in one or more databases
- Secondary use
- ***Examples:***
    - Marketplace: Household
    - Total Information Awareness

Encryption

- **Public key cryptography**
  - No need to communicate keys
  - Strong encryption: virtually impossible to figure out private key, given a public key

- **Pretty Good Privacy**
  - Phil Zimmerman created PGP (a public key encryption program); made it available on Internet
  - U.S. government threatened legal action

Electronic Money

- **An application of public-key encryption**.
  - When issuing electronic money,
    - a bank signs it with its **private key**.
    - **Customers** and **merchants** can use the **bank's public key** to verify the authenticity.
  - Bank **customers** can use their private key to withdraw funds.
    - The **bank uses** the **customer's public key** to verify the identity of the customer.
- ***Digital Cash*** – anonymous electric money
  - Relies upon blind signature protocol
  - Cannot trace back to the original buyer

Discussion

- Compared to people who lived 50 or 100 years ago, do you think we have more or less privacy today?

- Facebook, introduced “news feeds” and “mini- feeds” in 2006. Mini-feeds sent recent changes in a member’s profile to all the member’s friends. What’s your opinion on this?

Discussion Questions cont…

- Are you generally comfortable with disclosing personal info in exchange for free stuff?
- *Debate:* “Opt-in” vs. “Opt-out” policies in governing secondary use of information collected by merchants.

Thank you