Course Information

- Topics
- Work Schedule
- Grading
- Resources
- Academic Integrity
- Course Web page: https://www.cmpe.boun.edu.tr/courses/cmpe59b/
Privacy

- "Right to be let alone" (Warren and Brandeis, Harvard Law Review, 1890)
- "A state in which one is not observed or disturbed by other people." (Merriam-Webster Dictionary)
- "Someone’s right to keep their personal matters and relationships secret" (Cambridge Dictionary)
- "The right and ability of an individual to define and live his or her life in a self-determined fashion" (substantive privacy) (Dennedy, Fox, and Finneran, "The Privacy Engineer’s Manifesto", 2014)
  - By the individual
  - By others
  - By using the data about the person
Personal information

- Political opinions
- Sexual orientation
- Racial or ethnic origin
- Financial information
- Medical conditions
- ?
Properties of Privacy

- **Subjective:** May depend on the person
- **Contextual:** May change based on the context
  - **Time:** You don’t want your pictures taken at night to be shown
  - **Location:** You don’t want your pictures at the beach to be shown
  - **Culture:** You don’t want your pictures of eating meat to be shown in India
- **Purpose:** You don’t want to share your pictures if they will be used for advertising
- **Distributed:** May be e.g., in online social networks (OSNs)
What is privacy?

Privacy
The fair and authorized “processing” of Personally Identifiable Information (PII)

Processing includes collection, storage, use, organization, recording, alignment, combination, disclosure by transmission, consultation, erasure, destruction, alteration and so on...

Authorized = With Permission

Fair Information Principles
Collection Limitation
Data Quality
Purpose Specification
Use Limitation
Security Safeguards
Openness
Individual Participation
Accountability
+Privacy by Design & Generally Accepted Privacy Principles

Personally Identifiable Information
Formally: Any data that identifies an individual or from which identity or contact information of an individual can be derived
Practically: Includes otherwise non-personal information when associated or combined with personal information

Figure: "The Privacy Engineer's Manifesto", 2014
The Organization for Economic Cooperation and Development (OECD) Guidelines

- Collection Limitation: Should be collected lawfully and fairly
- Data Quality Limitation: Should be
  - relevant: Allow appropriate content to be accessed (e.g., age is relevant for checking credit history but phone number is not)
  - accurate: Allow owners to update if necessary
- Purpose Definition Required: Specify explicitly why that information is being shared
- Use Limitation Principle: How it is going to be used (e.g., share with third parties?)
- Accountability Principle: Data sharer will be kept accountable for not abiding with rules
Authorization Types

- Opt out (Default is to share)/Opt in (Default is not to share)
- Implied Consent (Your email address appearing on the instructor’s list for possible future communication)
- Informed Consent (Explicitly explained how and which information will be used)
- Expressed Consent (Explicitly specified by the user by checking a box or similar)
Real Life Scenarios

Real Life Scenarios

Real Life Scenarios

Real Life Scenarios

Real Life Scenarios

1

Lane v. Facebook: A Class-action lawsuit
- Sean Lane purchases a diamond ring from Overstock.com.
- This information shows up on the newsfeed of many of his friends, including his fiancee.
- This was result of Beacon app, with opt-out privacy options.
- Facebook ended up paying $9.5M
- Moral: Information propagates

Celebrity Stalking (from ABC News)
- iPhones embed picture locations into the picture (known as geotags)
- Geotags can easily be deciphered by apps, reveling the location even when not intended
- Not only bad for celebrities but for everyone
An Example with Propagation and Implication

lucy

charlie

linus
An Example with Propagation and Implication

lucy

friend

colleague: do not share location!

friend

charlie

linus
An Example with Propagation and Implication

- lucy shares location: at home
- charlie friend
- linus friend

Colleague: do not share location!
Problems

- Information is managed by users in social networks (as opposed to a single entity)
- Not enough to check the privacy agreement to preserve privacy of users
- Relations among users and inferences on accessible content may reveal private information
- Traditional access control schemes not working
- Privacy needs to be preserved at all times
Privacy Research Questions

- Allow users to specify privacy expectations (trust the OSN provider!)
  - Need for machine processable policies
  - Tools to check if policies are applied correctly or violated
- Enable users to agree on privacy settings before sharing
- Facilitate distribution of the social network (don’t trust a single authority)
- Learn users’ preferences and guide them in sharing content