Lecture 14: Authentication & Privacy

CS 181S

Fall 2020

Privacy concerns

- Humans might have concerns about measurements (have photo taken, parts of body scanned)
- Humans might not want to disclose attributes during enrollment (SSN, political party)
- Humans might not want action bound to their identity (buying medication)
- Humans might not want their actions linked to other actions, exposing them to inference about what they thought were unrelated activities.

Privacy and biometrics

- Biometrics can violate intrinsic privacy by requiring submission to bodily contact or measurement
  - Fear of germs
  - Religious prohibitions
- Biometrics can violate informational privacy
  - Biometric identifiers might effectively become a standard, universal identifier, enabling linking

Principles for privacy

- **Seek consent:** get permission to authenticate and store identity
- **Select minimal identity:** use the smallest possible set of attributes
- **Limit storage:** don't save information about identity or authentication without need, and delete when no longer needed
- **Avoid linking:** don't reuse identifiers across systems

Exercise 1: Facial Recognition

Complete the five readings posted on the course website, then answer the following questions:

1. What do you find to be the most convincing argument in favor of banning facial recognition systems?

2. What do you find to be the most convincing argument against banning facial recognition systems?

3. Would you recommend a national ban on the development and use of such systems?

Exercise 2: Feedback

1. Rate how well you think this recorded lecture worked
    1. Better than an in-person class
    2. About as well as an in-person class
    3. Less well than an in-person class, but you still learned something
    4. Total waste of time, you didn't learn anything

2. How much time did you spend on this video lecture (including time spent on readings)?

3. Do you have particular questions you would like me to address class?

4. Do you have any other comments or feedback?