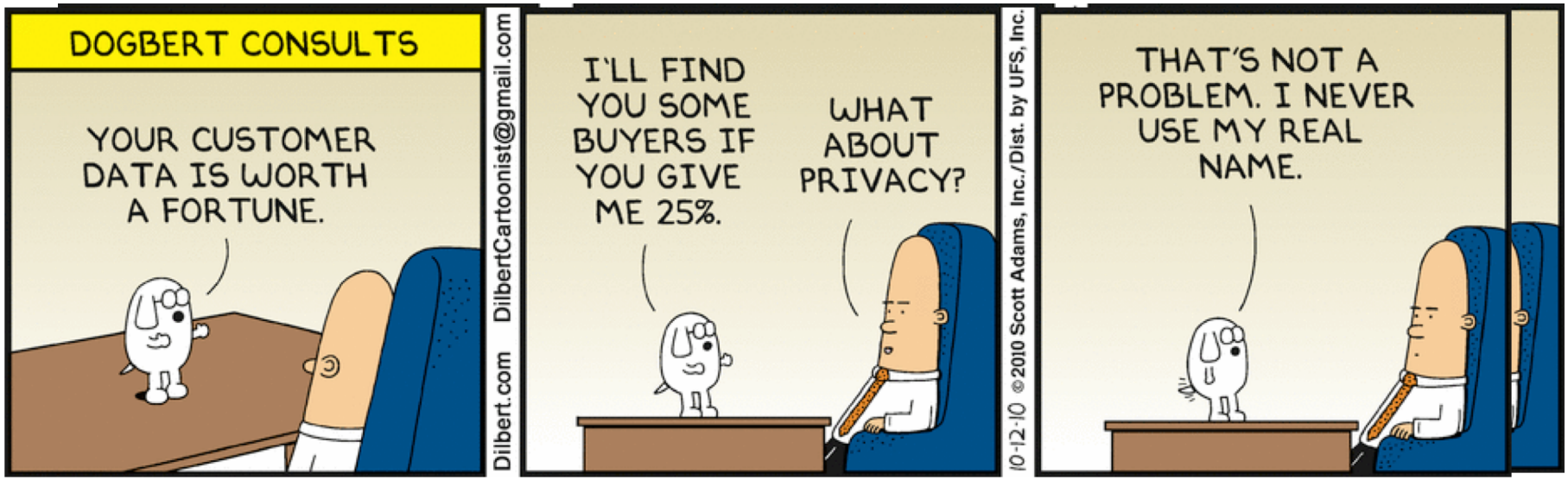
Lect. #18: Privacy 1



dilbert.com/strips/comic/2014-07-15/

Announcements

- GCS-PM plan due before 11:59 pm this Friday, 10.28.22
- No lecture on Tuesday, 11.15.22, so teams can work on GCS initial report
- Initial report then due before 11:59 pm on Friday, 11.18.22, last day before Thanksgiving break
- Questions?

Agenda for Today

1. What We Mean by Privacy

2. Examples of Privacy Issues

3. Nissenbaum's Privacy Model and Contextual Integrity

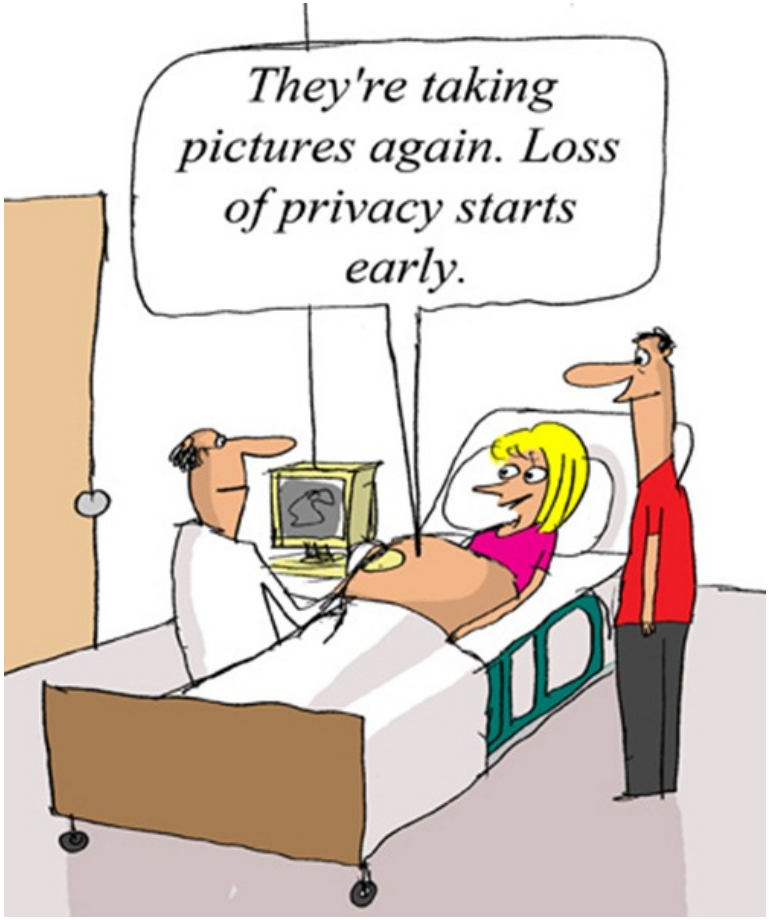
4: Application of Nissenbaum's Privacy Model

Privacy: What do we mean by it?

dictionary definition: freedom from unauthorized intrusion

- We can also think of privacy in terms of metaphors:
  - a *repository* of personal information that can be gradually eroded
  - a *personal space* that can be invaded
  - a *right* deserving legal protection that can be violated
- What is considered to be private varies from individual to individual, between cultures, and even over time

Privacy: Privacy vs A Right to Privacy



- We distinguish between:
  - Having *privacy*: descriptive/factual
  - Having a *right to privacy*: normative/opinion
- Again, what's considered a right to privacy also varies by individual, by culture, and over time

www.howtogeek.com/125574/geek-comic-for-september-30th-loss-of-privacy-starts-early/

Privacy: Loss of Privacy vs. Violation of Privacy Descriptive vs. Normative

Scenario 1: *Maria goes to the computer lab at 11 pm; no one else is there until 11:45 when Tom enters the lab to close it up for the evening. Tom sees Maria, and when she looks up from the computer, she's startled to see him gazing at her.*

Scenario 2: *Tom follows Maria from the computer lab to her apartment. After she's inside, he peeps through the keyhole in the door and watches her working on her laptop.*

Scenario 1: Maria has lost her privacy, but she was in a public place and, thus, had no expectation of preserving her privacy (descriptive privacy).

Scenario 2: Maria has lost her privacy, and her privacy has also been violated (normative privacy).

Poll

The EECS main office has open desks for staff. Would I violate a staff person's privacy if I looked for a pen on top of their desk to write them a note?

A. Yes

B. No

C. Other

Privacy: Evolution of Privacy in the U.S.

Privacy	Definition
Accessibility (19th and early 20th centuries)	Privacy is defined as one's (physically) being let alone or being free from intrusion into one's physical space
Decisional (1960s – 1970s)	Privacy is defined as freedom from interference in one's personal choices, plans, and decisions
Informational (1990s – present)	Privacy is defined as control over the flow of one's personal information, including the ways in which that information is collected and exchanged

Privacy: Why is privacy important?

- In 1999, the CEO of Sun Microsystems remarked to a group of reporters, “You have zero privacy anyway. Get over it.”
- In 2013, the CEO of Facebook stated that privacy “is no longer a social norm.”
- Despite these two claims, there are many arguments for why privacy is important:
  - It’s essential for such things as trust and friendship.
  - It’s an “expression” of the “core value” of security which is necessary for humans to thrive.
  - It plays a key role in promoting human well-being.
  - It serves to protect us from interference, coercion, and the pressure to conform.
  - It’s essential for democracy (assuming you support democracy).

Privacy: Why do *WE* (in EECS) need to care about privacy?

1. We deal with personal information in our workplaces including:
   - Client and customer personal information
   - Employee/colleague personal information
   - Employee/colleague data on work activities
2. We design and build new hardware and software technologies involving personal information including:
   - Collection
   - Storage
   - Analysis
   - Manipulation
   - Sharing

Breakout Discussion (4 min)

We design and build new hardware and software technologies involving personal information.

- In your breakout discussions, list technologies built by engineers (CptE, EE) and computer scientists (CS, SE) that are eroding our privacy
- We'll list some of the technologies after the breakout discussion

Privacy: Technologies that Are Eroding Privacy

- Mail calendars
- Cookies
- Ancestry DNA tests
- Proctoring software
- Rewards cards
- Smart phones
- GPS trackers
- Smart speakers
- Social media
- Algorithms used for preferences
- Health trackers
- RFID
- Tesla
- CCTV cameras
- Social credit systems and facial recognition
- Credit scores
- Drones
- Targeted advertising (selling data)
- Search engines
- Social technology

Poll

If a parent or grandparent checks your web browsing *history*, is it a violation of your privacy?

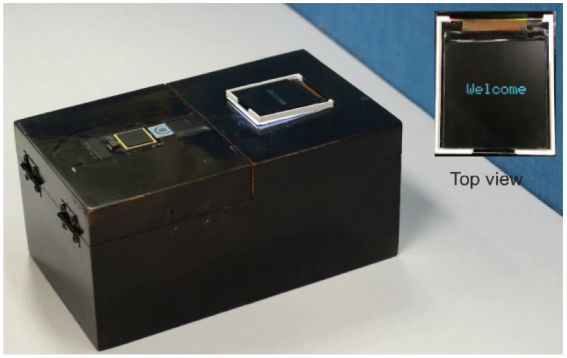
A. Yes

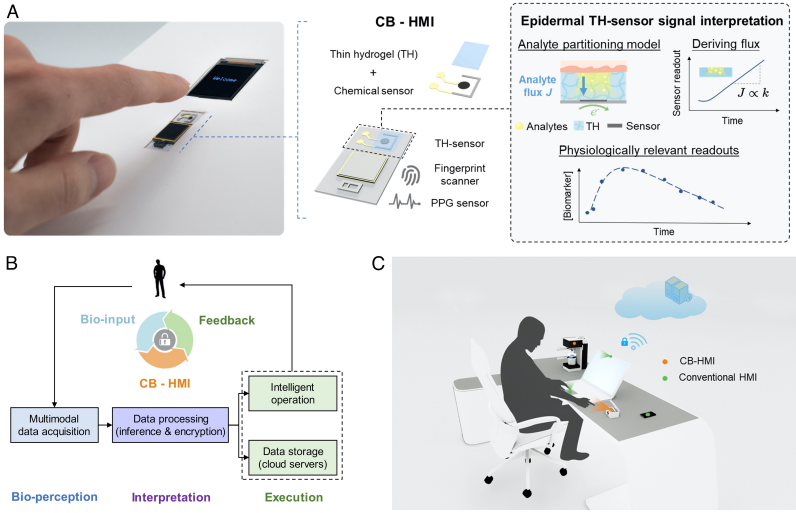
B. No

C. Other

Privacy: Privacy Issue?
Cryptographic Bio-Human Machine Interface (CB-HMI)

- CB-HMI, a secure, non-invasive, one-touch technology developed at UCLA and Stanford
- Presents detailed information about blood composition including metabolites, hormones, nutrients, and pharmaceu-ticals with a press of a finger
- Potential applications:
  - Embed in vehicle steering wheels to measure blood alcohol and drug levels
  - Relay real-time, detailed physiological information from patient to doctor during video visit
  - Incorporate into heavy machinery to ensure operators are authorized and physically sound





https://www.pnas.org/doi/10.1073/pnas.2201937119

Privacy: Privacy Issue?
Search and Rescue Drones

- UAV designed and equipped for rescue operations
- Used to search for lost or stranded people or to deliver supplies to people in need
- Used where unsafe or impractical for humans to access
- Key capabilities:
  - Cameras including IR and thermal
  - Several miles of range
  - Extended flight times
  - GPS tracking
  - Obstacle detection
  - Other sensors

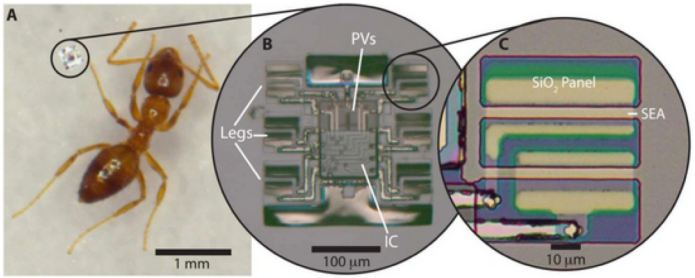
littleripper.com/best-drones-for-search-and-rescue/

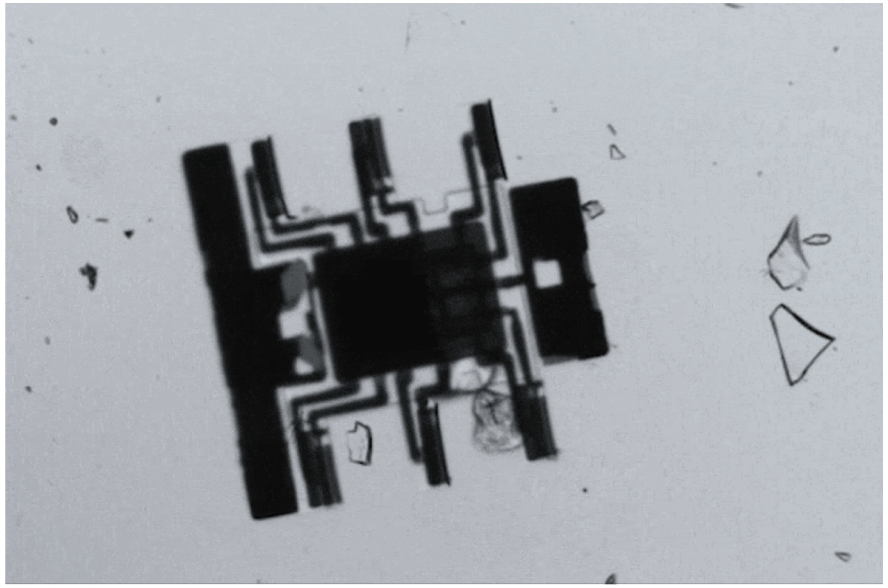
Privacy: Privacy Issue?
Wearables

- Demand for body-tracking wearables is strong
- Projected $14B spent on them in 2022, more than double spent in 2018
- Wearables include sport tech, smart watches, connected exercise equipment, health-monitoring devices, fitness trackers, and more
- Circular Ring introduced at the 2022 CES; competitor for OURA who is suing Circular Ring maker
- Circular Ring analyzes blood oxygenation, heart rate variability, temperature, heart rate, energy, cardio points, steps, resting heart rate, breathing rate, VO2 max, sleep cycles, recovery (some Garmin watches do as much if not more)

Privacy: Privacy Issue?
Antbots

- Antbots are the size of an ant *to* an ant; small enough to sit on a human hair and powered by light
- Not exactly a robot yet, but at least it's able to move autonomously
- Made of photovoltaic cell, integrated circuit, and set of hinged legs
- Not intelligent—yet!





Privacy: Privacy Issue?
Sensor that Measures Cortisol in Sweat

- Swiss research institute EPFL engineers and start-up Xsensio have developed a wearable sensing patch that measures cortisol concentrations in human sweat
- Sensor uses aptamers, short sequences of RNA or DNA, which immediately bind to cortisol when contact occurs
- Cortisol is secreted when people are stressed
- Measurement of cortisol concentration will allow objective way to quantify stress levels
- Stress can damage one's health, causing obesity, cardiovascular disease, depression, or burnout, so knowing stress levels is important

Poll

Which object/technique has the greatest potential for privacy abuse when not used as originally intended?

A. Cryptographic Bio-Human Machine Interface

B. Search and Rescue Drones

C. Wearables

D. Antbots

E. Stress sensor

Privacy: Nissenbaum's Model of Contextual Integrity

- Nissenbaum considers privacy within the notion of context in her model of privacy as contextual integrity
- Everything happens within a certain context
- Contexts include spheres of life such as schools, hospitals, workplaces, among family and friends, and so on
- Adequate privacy protection is linked to two norms of specific contexts:
  - Norms of appropriateness
  - Norms of distribution
- Contextual integrity, and thus privacy, is maintained when both norms are respected

Privacy: Norms of Specific Contexts

- Norms of appropriateness:
  - Is a given type of personal information appropriate or inappropriate to divulge within a particular context?
  - Example: Patient X's height, weight, blood pressure, glucose levels, and other metrics are determined at a hospital
- Norms of distribution:
  - Is the flow of information within or across contexts limited?
  - Example: Patient Y makes an appointment to see a specialist; the specialist requests the most recent medical records from Patient Y's physician, who forwards these to the specialist

Privacy: Hypothetical Scenario
Privacy Analysis Using Nissenbaum's Model

Suppose that, in your team's common workroom, you look over Lee's shoulder and notice that she's working on your team's code base. She's implementing a particular function that, in a recent team meeting, the project manager said was "low priority" and not to be implemented for another few months. You go immediately to the project manager's office and tell her that Lee is working on the "low priority" function.

Norms of appropriateness: Probably satisfied

Norms of distribution: Probably satisfied, but not necessarily the best way to handle things

Breakout Discussion (5 min)

Facebook's policy allowed Cambridge Analytica to obtain the personal information of 87 million FB users. Of these, only 270,000 had explicitly consented to download an app provided by CA, and they only agreed to have their data used for academic research. CA used the data to create profiles of the FB users which were sold to at least two politicians who used them to target ads for elections occurring in 2016.

- In your breakout discussions, use Nissenbaum's privacy model to determine whether contextual integrity was maintained, i.e., whether the privacy of FB users wasn't violated
  - Norms of appropriateness: Was personal information appropriately divulged in the context described above?
  - Norms of distribution: Was the flow of personal information limited within the context described above?

Poll

Do you think the U.S. needs a privacy law?

A. Yes

B. No

C. Other