CS 208 Embedded EthiCS Module, 10 March 2022
In-Class Activity Worksheet

You've now been introduced to Helen Nissenbaum's *contextual integrity* framework. Let's try using the framework to analyze a fictionalized case. Please read the case (below) and work with your group to answer the discussion questions that follow. We'll pause after each step.

Fictionalized Case: "Coachable"

Coachable is a technology company that designs wearable fitness trackers for athletes. Coachable trackers collect hundreds of data points per second about users' blood flow and temperature in order to measure their resting heart rate, heart rate variability, and respiratory rate throughout the day and night. These measurements are used to calculate metrics on users' sleep quality (including duration in bed, duration asleep, number of disturbances, length of time spent in different sleep stages, etc.), the level of strain (i.e., physical and mental stress) put on their body, their recovery rate and readiness for activity, and their overall cardiovascular health.

In order to learn how different factors affect their training and performance, users log their behaviors and demographic traits in the Coachable journal. Coachable provides over 100 categories in which users can log information, including:

- Alcohol and marijuana consumption
- Supplement use and dosage
- Caffeine consumption
- Medications and sleep aids
- Screen time and bedtime routines
- Air travel
- Stretching and other recovery modalities
- Nutrition and diet plans
- Menstruation and pregnancy

One of Coachable's newest features is allowing users to understand the effect that sexual activity and arousal has on their training and recovery. This allows them to adjust their sexual activity as needed to optimize their athletic performance. The Coachable journal now prompts users to enter information about:

- When, where, and with whom they engage in sexual activity

Coachable users receive detailed reports on how the behavior logged in their journal affects their athletic training, along with personalized training plans, lifestyle tips, and audio-guided workouts.

Coachable collects and stores all user data in a centralized database and uses it internally to analyze and improve its products and services, add features, and better understand its users' needs. Coachable does not share or sell raw user data directly to third parties. However, it allows other parties, including advertisers and sports recruiters, to perform differentially private queries on user data for their own purposes, within the confines of the law. Queries are rate-limited and/or registered beforehand.

Discussion Questions:

STEP 1: EXPLAIN

Step 1 involves describing how, if at all, Coachable's practices disrupt the way that information normally flows in the relevant social context. Let's start by considering how information flows in the case as described above (Q1).

Question 1: The diagram below features some key actors in the case. For each actor, consider *whether* personal information flows between that actor and the others. If it does, consider *what kind* of information flows and *how* it flows (e.g., Is it compelled or voluntary? What purpose is it used for? Is it ever bought or sold? Is it kept confidential beyond that point?)

Next let's locate a relevant social context that has a similar *function* or *purpose*. This is the context that the technology we're analyzing serves as an extension of. For today, let's say the relevant context is the **athlete-coach relationship.** Of course, there's *no actual coach* in the Coachable case. However, the app serves a similar function to that of an athlete's coach.

Question 2: In the context of a good athlete-coach relationship, what kind of information flows between whom, and how does it flow? (Draw your own diagram)

Next, let's identify disruptions (Q3)

Question 3: How does the flow of information in the case differ from the flow of information that we normally expect in the context of an athlete-coach relationship? In other words, how is your diagram in Question 1 different from your diagram in Question 2?

Finally, let's consider what role differential privacy is playing in the analysis (Q4)

Question 4: If Coachable did *not* use any differential privacy techniques in answering third parties' queries, how would information flow differently in the case? (How would your Question 1 diagram differ?) Would there be any additional disruptions? (Would your answer to Question 3 change?)

STEP 2: EVALUATE

According to *contextual integrity*, the fact that a technology or practice disrupts the normal context-specific flow of information provides *a reason for suspecting* that it violates privacy. Step 2 involves evaluating the disruptions that you identified in Step 1, Question 3 to see if they serve general and context-specific values and goals.

Question 5: What (if any) individual values might be relevant? (Consider: What do Coachable users want? What would be good for them?)

Question 6: What (if any) societal values might be relevant? (Consider: How might Coachable's data practices affect distributions of power, resources, and opportunities across groups?)

Question 7: What are some of the values and goals specific to the coaching context or the athlete-coach relationship?

Question 8: Based on your answers to Questions 5-7, do you think the disruptions you identified in Question 3 support general and context-specific goals and values?

STEP 3: PRESCRIBE

Question 9: Based on your answer to Question 8, should Coachable change any of its data collection or use practices? Why or why not?

Questions? Contact Sophie Gibert at sgibert@g.harvard.edu