CS 5436 / INFO 5303 Fall 2024
<u>Homework 3</u>

Due: November 12, 11:59p ET

This is an INDIVIDUAL assignment.
You may discuss but each student must submit their own work.

REQUIRED (40 points)

Problem 1 (2 points)
Use https://banthescan.amnesty.org/decode/ to calculate the number of surveillance cameras on your route home from the Cornell Tech campus (if you live on campus, use your favorite restaurant in Manhattan as the destination).

Problem 2 (4 points)
(a) Explain, at the technical level, how services like Clearview AI and PimEyes work, and why their technical architecture gives them a plausible defense against accusations that they violate privacy.

(b) Identify and discuss at least three ethical or privacy concerns associated with the use of Clearview AI's facial recognition technology.

Problem 3 (6 points)
(a) Surname inference for anonymous genomes is similar to re-identifying anonymous datasets by record linkage. There is, however, an additional aspect of anonymous genomic data that makes it especially vulnerable to (re-)identification. What is it?

(b) What is the key type of auxiliary data for identifying anonymous genomes? How does the use of this data fundamentally rely on your answer to Problem 3(a)?

(c) Gymrek et al. paper on surname inference mentions meiosis. What is meiosis, and why is it important for identifying anonymous genomes? In your answer, refer to your answers to Problems 3(a) and 3(b).

Problem 4 (6 points)

(a) Why has consent been considered so important (perhaps essential) in prevailing privacy regulations in the US and elsewhere?

(b) What role does anonymity play in the privacy landscape?

(c) Provide two reasons why anonymity is important in free societies?

(d) Explain the metaphor of "end run" applied to anonymity and consent.

Problem 5 (6 points)

For each of the cases, answer the following questions (based on lecture and course readings):
i) What are the potential legal issues
ii) Which area of law seems most relevant?
iii) In your view, is the action in question legal (Yes/No/Depends)
iv) What are the main reasons for your choices?

(a) Cornell sells student transcripts to a headhunting firm.

(b) Coursera sells performance information about you to a headhunting (recruitment) firm.

(c) Acxiom (a data broker) obtains divorce records from the New York State Courthouse

Problem 6 (8 points)

(a) (i) Briefly describe key elements of the video that Dr. Geddes showed in class.

(a) (ii) Among several elements of 4th Amendment protection that were raised in the video, briefly describe two.

(b) Briefly describe the original scope of the 4th Amendment.

(c) (i) Define "reasonable expectation of privacy" and (ii) explain how it extends the original scope, per your answer in (b)

Problem 7 (5 points)

Note: We will grade on the basis of how you apply the test, less so on the specific answer.

(a) List all elements of the Katz-Carpenter Test

(b) How could you use it to decide if the government would need a warrant to gain access to:
(i) 10 years of chat records (e.g. from Meta or iChat)

Problem 8 (2 points)

(a) What is a tort?

(b) List two ways, discussed in Ben Sobel's lectures, in which Tort law is different from other areas of law.

Problem 9 (1 point)

Ben Sobel used an example involving horse drawn carriages. Briefly explain the point he was making.

PICK YOUR OWN – should add up to **20 points**
For each problem you pick, do the entire problem (i.e., you cannot choose-and-mix subproblems)

Problem CS1 (8 points)

Implement a prototype face recognition system following this tutorial and evaluate it on any publicly available dataset of labeled face images (other than the one in the tutorial). Submit your code and test cases.

What accuracy did your recognizer achieve?

Problem INFO1 (2 points)

Photography using Daguerreotype technology (circa 1839) required subjects to quietly pose for as long as 15 minutes. In 1890 Warren and Brandeis argued that "instantaneous photography violates privacy, (One of the most famous sentences in their article, *The Right to Privacy,* "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life and numerous mechanical devices threaten to make good on the prediction that what is whispered in the closets shall be proclaimed on the rooftops.") Use CI to pinpoint two sources of privacy disruption.

Problem INFO2 (3 points)
ANSWER ONLY THE UNDERLINED PORTION: you have already answered (a) and (b)(i)
Note: We will grade on the basis of how you apply the test, less so on the specific answer.

(a) List all elements of the Katz-Carpenter Test
(b) How could you use it to decide if the government would need a warrant to gain access to:
     (i) 10 years of chat records (e.g. from Meta or iChat)
     (ii) 3 months of drone surveillance footage of an individual as they go about their day

Problem INFO3 (4 points)
ANSWER ONLY THE UNDERLINED PORTION: you have already answered (a) - (d)

(a) Why has consent been considered so important (perhaps essential) in prevailing privacy regulation in the US and Europe?
(b) What role does anonymity play in the privacy landscape?
(c) Provide two reasons why anonymity is important in free societies?
(d) Explain the metaphor of "end run" applied to anonymity and consent.
(e) Briefly explain how the End Run argument (specifically) exposes a problem:
     (i) with treating anonymity as a privacy solution.
     (ii) with treating consent as sufficient for protecting privacy.

INFO4 (2 points)

(a) In the US, The Privacy Act of 1974 was a major disappointment. Why?

(b) The Bill of Rights is severely limited in its protection of privacy. Explain.

INFO5 (3 points)

(a) Why is the US's approach to privacy regulation called sectoral?

(b) Name two sectoral laws and briefly say what they regulate

Problem INFO6 (8 points)

(a) Specifically referring to the Target case, explain how a company can make an "end run" around consent.

(b)(i) Briefly describe how an adherent of CI might, in specific cases, counteract an end-run around anonymity.

(b)(ii) Barocas & Nissenbaum cite work of Neil Manson and Onora O'Neill to compare and contrast informed consent in biomedicine and consent as embodied in privacy policies for digital services and websites. What approach do they draw from these observations to counteracting the challenges of end run around consent?

Problem INFO7 (3 points)

(a) List Prosser's four privacy Torts

(b) Briefly illustrate one of them from examples Ben Sobel discussed in class

Problem INFO8 (1 point)

Tort law is one of the approaches the law offers for seeking redress for privacy harms. Yet, as noted in class, it poses challenges in its use. Briefly explain one.