MACS Assignment 8
Neta Grossfeld
December 3, 2018

Question 1: Identification risk in anonymized data (4 points).

The examples of health insurance data and the Netflix movie rating data have very similar structure regarding re-identification attacks. In the health insurance data, Latanya Sweeney received the health insurance dataset and sought out another, public dataset of voting records. These datasets shared common information, such as Zip Code, Birth Data, and Sex. From those three shared variables, Sweeney was able to identify and match the health insurance records to the public voting records, providing personal information including name and home address which had previously been removed from the health insurance data before being released.

In the Netflix movie rating example, the “anonymized” movie ratings, even with additional small changes to the data, the structure is similar in that another publically available data source, another movie rating system called IMDb, had the ability to match with and identify a large group of individuals in the dataset released by Netflix. In both examples, a publically available dataset was able to be linked with and reveal personal information from the “anonymized” datasets.

The linked datasets for the two examples mentioned above have the potential to reveal sensitive information about people that may be ruinous. For example, potential employers may be able to check the linked health insurance dataset to check candidates’ medical records and determine to pass on a position based on expensive health risks or pregnancy. This would result in an economic risk for the individual candidate. In the Netflix example, a lawsuit was brought against them claiming information risk including economic, social, and psychological risk affecting certain individuals. The reason for this claim is that movie preferences can be extremely revealing of a person’s true identity and may cause shame or ridicule if others were aware.

Question 2: Describing ethical thinking

Kauffman uses more of a consequentialist viewpoint rather than a deontological one when he makes the point that “sociologists generally want to know as much as possible about research subjects.” In this case, he is saying that the dataset is of better use for research if certain data is included, and is less worried about the deontological case, or that ethical duties

would require him to remove that particular data before releasing. It seems Kauffman also believed that the risk was rather low compared to the benefit under the principle of beneficence since he comments that the information was already available on Facebook if someone wanted to find it. He also argues compliance, from the respect for law and public interest principle, with the common rules and regulations at the time, including approval from the IRB.

Question 3: Ethics of Encore

The Encore program, a computer science research program, was used to measure censorship across the globe by adding a line of code to web browsers. However, users of the web browsers were not informed that their IP addresses were being used to detect censorship. Authors Narayanan and Zevenbergen assess Burnett's and Feamster's Encore web censorship study using mainly the structure and principles outlined in the Menlo Report, one analytical framework used to define and regulate scientific ethics.

In accordance with the Melo Report, the authors first attempt to investigate the stakeholders involved in the study, which is essentially any Internet user. The researchers of the study promote this as proof of scalability, which is actually desired in the field of computer science. This highlights the conflict between established ethical principles and the consequentialist values upheld by the technology industry. In addition, these researchers and other computer scientists view this study as research on technical systems, or censorship, as opposed to human subjects, the users. The Princeton and Georgia Tech IRB also don't recognize this study as one of human subjects, in accordance with the Common Rule.

The authors then perform a beneficence analysis, where they discuss the benefits and harms of the study. The major benefit of this study is that the collected data can help identify the motivation behind a censorship, as well as the technologies used to censor. This data can lead to understanding what information a government might censor and why, and also provide a way to possibly reverse-engineer the government's censorship capabilities. One potential harm is that a user may be identified via their IP address, which could lead to government punishment depending on the site visited by Encore and the reason why the site was censored. However, Encore limited the URLs being visited to only those for major social media sites, where access is commonly sought. Given this risk/benefit analysis as per the Menlo Report, the authors concluded that this study contributed significantly more benefits than risks, especially when controls were enforced to mitigate those risks.

Next, the authors review the issue of informed consent, transparency, and legal compliance. The researchers argue that informed consent would be impractical and unfeasible due to the global scale and measurement approach of the study. This again represents a consequentialist framework since the researchers are focused more on the measured result of the study that would benefit those affected by censorship on a grander scale, rather than the ethical duty of seeking informed consent from all the users required for the study. To increase transparency, the authors argue that the researchers could provide greater access to an opt-out option. In regards to legal compliance, the authors confirmed that the researchers are acting within U.S. regulations, but the same confirmation cannot be provided for the other countries that Encore operates in. This could prove harmful to certain individuals, yet the researchers' consequentialist tendencies justify the study for themselves and others.

Overall, I agree with the authors' assessments of the Encore web censorship studies' ethical quality. Specifically, the restriction of URLs to common social media sites removes my concern for individuals who may be unwittingly attempting to visit sensitive sites from their IP addresses, which could lead to government suspicion. Additionally, I agree that the researchers could make the opt-out option accessible, with clear information and the program and its potential consequences. To me, this seems to be an alternative to informed consent, since at least the participants could be aware of and have the capability to remove themselves from the study.