Assignment 8

MACS 30000

Jiaxu Han

1. Identification risk in anonymized data.

(a)

Salganik proposed that "it is wise to assume that all data are potentially identifiable and all data are potentially sensitive" (2018, section 6.6.2) because there is a higher informational risk in digital-age research. For example, the Netflix movie rating data that we discussed in an earlier assignment and health insurance records from Group Insurance Commission (GIC) both have a high risk for "re-identification attacks" (Salganik, 2018, section 6.6.2) proved by researchers.

Both re-identification attacks shared a similar structure where the dataset being "attacked" and having "no obviously identifying information" is linked to an auxiliary dataset which contains people's identities (Salganik, 2018, section 6.6.2). In addition, neither of the dataset itself was capable of releasing sensitive information, but they had shared attributes linking which would allow personally identifying information matched to records in "anonymized" dataset. Finally, both auxiliary datasets were relatively accessible to the general public, which render the original datasets that contain very sensitive information even a higher risk of leakage. For example, Sweeney who was a graduate student paid $20 to get the voter registration list for Cambridge Massachusetts that was linked to health insurance data (Sweeney, 2002, p558); and Narayanan and Shmatikov (2008) obtained auxiliary information from subscribers' public ratings at Internet Movie Database (IMDb).

(b)

As mentioned above, Sweeney (2002) used voting registration data which was relatively accessible to re-identify the "anonymized" medical records. Zip code, birth date, and sex were three shared variables in those two datasets (Sweeney, 2002). Though only three shared attributes, they were able to create a "unique fingerprint" (Salganik, 2018, section 6.6.2). Then, Sweeney was able to use them to match the person in the voting records to his/her medical records which contain visit date, diagnosis, procedure, and medication. Therefore, although the medical record dataset released by GIC was "anonymized" by taking out names and home addresses, it still has a risk of revealing sensitive information by linking it with another dataset. As an example, Sweeney identified William Weld's medical record who was governor of Massachusetts at that time (Sweeney, 2008, p559).

Similarly, Narayanan and Shmatikov (2008) merged the Netflix rating data with some public profiles on IMDb. Narayanan and Shmatikov (2008) proved that if a subscriber rated on both services, it was "sufficient to identify his/her record in the Netflix Prize dataset" (p12). They expected that if an IMDb user gave a public rating on a movie, they would give a similar rating score on the same move privately on Netflix (Narayanan & Shmatikov, 2008). Thus. the shared rating scores would allow researchers to re-identify the records in Netflix dataset. They picked around 50 IMDb users to demonstrate their idea. After cleaning the data and applying their

algorithm “Scoreboard-RH” (see Narayanan & Shmatikov, 2008, p5 for details) on the datasets, they were able to identify the records of two users in the Netflix dataset with eccentricities of around 28 and 15, which are very strong matches (Narayanan & Shmatikov, 2008, p13).

2. Describing ethical thinking.

Kaufman and colleagues (2012) conducted a study called “Tastes, Ties, and Time” (T3) to investigate social networks and cultural tastes by scraping facebook profiles of the class of 2009 at a private college and they made their dataset public afterward (Salganik, 2018, section 6.2.2). Soon after the data were made available, other researchers were able to not only deduce that this study was conducted at Harvard college but also re-identify some students in the dataset (Zimmer, 2010), which instigated a lot of discussion about ethical issues about this study.

The main ethical concern related to T3 study is a privacy violation, as mentioned by Zimmer (2010, p321) “the failure to properly mitigate what amounts to violations of the subjects’ privacy, and thus, the failure to adhere to ethical research standards”.

Zimmer cast doubts about the “improper access to personal information” via “using research assistants from within the Harvard to community” to collect Facebook data without consent (Zimmer, 2010, 322). In response to that, Kaufman, the principal investigator of the T3 project, commented that “what might hackers want to do with this information, assuming they could crack the data and ‘see’ these people’s Facebook info? Couldn’t they do this just as easily via Facebook itself? Our dataset contains almost no information that isn’t on Facebook.” (Sep. 30, 2008c). He was trying to defend himself that the Facebook profile is public anyway and so there seems no reason to obtain consent from each one of the students in an extensive dataset. However, such a rationale violates the principle “respect for persons” (Salganik, 2018, section 6.4.1) that they used their data without obtaining corresponding consent. Though the Facebook profile is public, it is not equal to a consent for granting use for any research purposes.

Kaufman partially admit that it was lack of consideration of privacy issue when releasing the data but partially defend himself by saying “we’re sociologists, not technologists, so a lot of this is new to us” (Sep.30 2018c) and “we did not consult w/ privacy experts on how to do this, but we did think long and hard about what and how this should be done” (Sep.30 2018b). Kaufman may not aware of the risk of re-identification and potential harm of students in the dataset, but it is a researcher’s responsibility to adhere to the principle of “beneficence” and thus “put extra safeguards in place when they released the data” (Salganik, 2018, Section 6.4.2).

Kaufman probably considered the balance of risks and beneficence by releasing the data: “We thought long and hard about what to do with the unique ‘Favorite’ listings – they do indeed have the potential to compromise subjects… though they will be enormously useful to researchers interested in taste, culture, etc. Our other option would be to replace taste names with numbers, but then researchers will only know how many tastes people have in common, not what those tastes are” (Sep. 30 2008b). However, the consequence would be that “one group of students

bore the burdens of the research and only society as a whole benefited" and that compromises the principle of "justice" of the T3 project (Salganik, 2018, section 6.4.3). Kaufman's comment about the decision of releasing data to benefit more researchers also reflected "consequentialism" thinking of the ethical framework (Salganik, 2018, section 6.5). However, in this case, benefiting society should base on doing no harm to students whose many private information was stored in the dataset.

3. Ethics of Encore

(a)

Encore is "a computer science research project in January 2015 executed code on the web browsers of unsuspecting users to detect censorship worldwide including in China and Iran" (Narayanan & Zevenbergen, 2015, p1). Two researchers, Narayanan and Zevenbergen, then conducted a detailed ethical evaluation of the Encore project in five dimensions.

First, Narayanan and Zevenbergen provided an "ethical inspection" which raises questions of "who the stakeholders are and whether Encore is human-subjects research" (2015, p8). However, there are no straight answers to these two questions and the analysis conducted for these two questions revealed the complex interplay between ethics and the technical design of the experiment. For example, when identifying the stakeholders, the goal of scalability of the Encore project and in computer science, in general, is conflicted with general human research goal of "minimizing the number of subjects necessary to measure a given effect with statistical rigor" (Narayanan & Zevenbergen, 2015, p9). As a result, the worldwide scale of Encore makes analyzing potential stakeholders individually almost impossible (Narayanan & Zevenbergen, 2015, p9). Similarly, there were also some debates about whether researches like Encore project is human-subjects research, which hasn't reached consensus and complicates the ethical issue associated with this project.

Second, Narayanan and Zevenbergen followed the "consequentialist thinking" by focusing on the balance of potential benefits and harms in the "principle of beneficence" (Salganik, 2018, section 6.5) for Encore project. The benefits of the research include understanding the motivations and the technologies behind censorship and thus "enhancing the ability to create effective censorship circumvention tools" (Narayanan & Zevenbergen, 2015, p11). On the other hand, due to the scale of Encore project, it was difficult to anticipate harms for each individual and thus to strictly adhere to the requirements of the beneficence principle for a small research group (Narayanan & Zevenbergen, 2015, p11). Depending on the type of censored website, individual may face the different magnitude of risks. In addition, when researchers in Encore group knew so little about rules of law in different countries, it was difficult to anticipate whether an individual would face persecution or any other form of harm by accessing to certain domains (Narayanan & Zevenbergen, 2015, p14). Narayanan and Zevenbergen did admit that the Encore researchers took actions to mitigate harm by limiting tests on only regularly accessed domains such as Twitter, Facebook, and YouTube, but there were still more questions for investigators to consider (2015, p14).

Third, Narayanan and Zevenbergen discussed the ethical concern about obtaining informed consent from users. Again, due to the scalability of the project, obtaining informed consent from each user was very challenging. However, it does not justify the Encore team's decision of not obtaining consent from its users and not require sites to inform its users about Encore. These conflicts again "highlights the tension between the scalability imperative and established ethical norms" and requires further discussion and research in the ethical issue in digital-age.

Finally, the paper discussed the legal compliance of the Encore project. Though the Encore team is based in the U.S. and in compliance of U.S. laws, the measurements took place worldwide and thus "makes the issue of jurisdiction unclear" (Narayanan & Zevenbergen, 2015, p15).

(b)

In my opinion, the main ethical concern about Encore project is the lack of informed consent for visitors of certain websites that installed the code snippet, which violates the principle of respect for persons. Having their browsers installed a snippet is definitely not what most users expected, nor is what they would want if they knew. In addition to that, the potential harm imposed on its users without their awareness and consent also violates the principle of beneficence. Burnett and Feamster admitted in their paper that "the risk that Encore poses are far more nebulous: laws against accessing filtered content vary from country to country, and may be effectively unenforceable given the ease with which sites (like Encore) can request cross-origin resources without consent; there is no ground truth about the legal and safety risks posed by collecting network measurements" (Burnett and Feamster, 2015, p663). Acknowledging the potential risks for its users, the Encore team did take actions to mitigate harm (see Burnett and Feamster, 2015, Table 2 for details). They followed "consequentialism" ethical framework by trying to balance the benefits and risks in this project. In "consequentialists" thinking, though the users who were exposed to potential harms may benefit from this research in the long run, researchers in this community shouldn't stop at where they are right now. Technical difficulty or lacking ethical rules for this kind of research are the challenges researchers need to tackle, but they are not the justification for never trying to obtain informed consent in the future.

Indeed, the ethical issue for the Encore project is very complicated. In fact, due to the development of computer science, researchers may face many new ethical questions that "conventional ethical standards do not address" (Burnett and Feamster, 2015, p663). Therefore, the Encore project provides a good opportunity for ongoing discussions about ethical issues related to computer science experiment similar to this and gradually establish a better ethical system in the community.

References

Burnett, Sam and Nick Feamster, "Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests," 2015.

Kauffman, Jason, “I am the Principle Investigator...,” Blog Comment, MichaelZimmer.org, http://www.michaelzimmer.org/2008/09/30/ on-the-anonymity-of-the-facebook-dataset/, Sep. 30, 2008b.

Kauffman, Jason, “We did not consult...,” Blog Comment, MichaelZimmer.org, http://www.michaelzimmer.org/2008/09/30/ on-the-anonymity-of-the-facebook-dataset/, Sep. 30, 2008c.

Narayanan, Arvind and Bendert Zevenbergen, “No Encore for Encore? Ethical QUestions for Web-based Censorship Measurement,” Technology Science, Decem- ber 15 2015.

Salganik, Matthew J., Bit by Bit: Social Research in the Digital Age, Princeton University Press, 2018.

Sweeney, Latanya, “K-Anonymity: A Model for Protecting Privacy,” International Journal on Uncertainty Fuziness and Knowledge-Based Systems, 2002, 10 (5), 557– 570.

Zimmer, Michael, “But the Data is Already Public: On the Ethics of Research in Facebook,” Ethics and Information Technology, 2010, 12 (4), 313–325.