Assignment #8

MACS 30000, Dr. Evans

Dongcheng Yang

1. Identification risk in anonymized data

(a) The two examples that I choose are the health insurance data case from Sweeney (2002) and the Netflix movie rating data case from Narayanan and Shmatikov (2008). Both cases reveal a similar structure of re-identification attack. In the dataset which contains the sensitive information, personal indentifying information such as names are deleted. There is also another dataset which contains personal indentifying information but does not include sensitive information. However, these two dataset share several variables. Thus, when they are merged together, sensitive information is revealed.

(b) In the health insurance data case from Sweeney (2002), there is one seemingly "anonymized" dataset containing individuals' medical information like the visit data, diagnosis, procedure and demographic information such as zip code, birth date, ethnicity, and sex. The procedure of anonymizing only revolves around deleting personal names and addresses. Besides, there is also another voting records dataset which includes information of birth date, gender, zip code and also names. Then, by merging these two dataset with demographic information as reference, sensitive medical information of a specific person could be identified.

In the Netflix movie rating data case from Narayanan and Shmatikov (2008), the situation is quite similar. Individual names are removed before the release of dataset containing ratings. However, there was still possibility that specific people's preferences over movies could be revealed. Narayanan and Shmatikov pointed out that anyone who has limited information of one specific person's preference of several kinds of movie could potentially get access to all of the person's ratings. Those limited

information serve as the identifier which leads to the emergence of the person behind. Although movie preference might not be sensitive information, personal attitudes towards sexuality, political issues could be.

2. Describing ethical thinking

Kaufman (Sep.30, 2008b) mentions the sociologists' general aim to grasp more information about the research topic and unfamiliarity with respect to the technology. The principle of beneficence describes the tradeoff between "maximizing benefits and minimizing harms" (Salganik, 2018, Ch.6). It seems that this optimization problem has no perfect solution when it comes to a specific research project. A good method to minimize harms might be to consult technical staffs before the release of the dataset.

Kaufman (Sep.30, 2008b) also points out that their dataset only includes information on Facebook. If the potential hackers are interested in those information, they could fulfill their needs directly from Facebook. That is to say, the information gathering process of building this dataset does not have any influence on the leakage of Facebook information. Based on the framework of "consequentialism" (Salganik, 2018, Ch.6), if the consequence does not change at all, the research team should not be blamed for any method they have taken advantage of to build such dataset.

Kaufman (Sep.30, 2008c) indicates that there was neither interview nor disclosure of personal information during the research process. They have followed the principle of "respect for persons" (Salganik, 2018, Ch.6) in this research and they made every effort to protect the dataset from being cracked. Thus, under the framework of "deontology", if the means in the project has little room for improvement, the researchers have accomplished their ethical missions. And it will be the hackers' fault to crack the dataset.

3. Ethics of Encore

(a) Narayanan's and Zevenbergen's assessment of the Burnett and Feamster (2015) Encore study uses the principles and framework in Menlo report as the baseline (Narayanan and Zevenbergen, 2015, p11). The principles of beneficence, justice, and respect for persons, law and public interest have all been taken into consideration.

Menlo report puts emphasis on the "stakeholder analysis". However, based on the research design of Encore study, it seems impossible to conduct the stakeholder analysis. Besides, conflicts remain among scholars about whether Encore is a "human-subjects research". The internet users might not be viewed as direct victims of the sociotechnical study, but the indirect negative effects exerted on them could not be neglected (Narayanan and Zevenbergen, 2015, p13).

The principle of beneficence entails the pursuit of balance between risk and benefits. In the Encore study, benefit revolves around the illumination of technologies and incentives behind censorship (Narayanan and Zevenbergen, 2015, p15). As for the risk aspects, the situation seems to be more complicated. Under the framework of "consequentialism" , the research team of Encore measures the risk of the project as compared with normal internet usage and claims that Encore does not impose more risk in people's daily life (Narayanan and Zevenbergen, 2015, p17). However, Narayanan and Zevenbergen mentions three other transmission mechanisms that might cause more risk. Firstly, there is a mismatch between users' awareness and the improved technology and this fact is often ignored by the researchers (Narayanan and Zevenbergen, 2015, p18). Secondly, when it comes to different kinds of websites, huge uncertainties exist with respect to severity of harm (Narayanan and Zevenbergen, 2015, p18). Thirdly, Encore research team has not taken the collective internet disconnection as a potential consequence (Narayanan and Zevenbergen, 2015, p19).

Some legal considerations are also put forward by Narayanan and Zevenbergen. Encore researchers could not be exempted from the risk of breaking the law because of the inconsistency of legal system in the world (Narayanan and Zevenbergen, 2015, p22).

(b) Based on the four principles and two frameworks in Salganik (2018, Ch. 6), the overall ethical quality of the Encore study should be questioned. Firstly, there seems to be no adequate respect for persons entailed in the project. Although it could be costly to ask people's permission every time Encore directs the browsers to some potentially censored websites, it is web users' fundamental right to realize the potential risk and make their own decisions. Secondly, censorship is an essential area which is quite in short of deep research, but Burnett and Feamster's research method is still too risky. If the users involved happen to live in the place which has strict supervision on network using, the corresponding harm behind this project might be too huge. The huge damage could even drive down the benefit risk ratio to nearly zero.

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.

__ , "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*, December 15 2015.

__ and Vitaly Shmatikov, "Robust De-Anonymization of Large Sparse Datasets," 2008.

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.