1.(a) In Montjoye et al. (2015), the author studied “the reidentifiability of credit card metadata” and gave examples about re-identifying information by linking other data to the credit card data (Montjoye et al., 2015, p. 536). In particular, “the risk of reindentification” was increased “by 22%” if “the price of a transaction” is known (Montjoye et al., 2015, p. 536). Zimmer (2010) discussed about the re-identification of college students’ Facebook data and the re-identification attack in his paper shows a similar structure of linking the data to other public databases.

(b) In Montjoye et al. (2015), for example, if we want to find the information of a person in a “simply anonymized credit card data set” and we know the places he visited in two days, we could simply look through the credit card dataset and identify the person visited these places on these two days. If there’s only one person satisfying this condition, we could re-identify this person’s information.

According to Zimmer (2010), the Facebook dataset includes sensitive housing, demographic, cultural, relational information of the students, which combined together could be used to identify the individual student. In addition, using the information in the descriptive codebook alone could identify the college in the dataset as Harvard College.

2.

Firstly, Kauffman’s team adopted the Beneficence principal proposed in Salganik (2018). On one hand, Kauffman believed that acquiring “as much as possible about research subjects” would benefit sociological research (Kauffman (Sep. 30, 2008b)). On the other, the team considered the potential harm to the privacy of the students and made the data anonymized to protect the students’ privacy. Therefore, both benefits and harms are evaluated in the T3 research project, which is in line with the Beneficence principal.

According to Kauffman, if hackers want to obtain the data, they could easily get it from Facebook directly, which means extracting the data wouldn’t increase the risk of exposure of privacy, which is in line with the principal of Justice in Salganik (2018). This argument also shows a consequentialism view as whether the researcher extracted the data from Facebook wouldn’t increase the potential harm to privacy.

In addition, the team obeyed the Respect for Persons principal in Salganik (2018) as they only accessed information available on Facebook and didn’t interview the students directly and made that information public. In this case, the privacy of students is not harmed, and the team respected the autonomous of the students.

3.(a)

In January 2015, Burnett and Feamster conducted a research project name “Encore”, which “executed code on the web browsers of unsuspecting users” to measure censorship worldwide (Narayanan and Zevenbergen, 2015, p. 1). Although this project brought “valuable information about the censorship activities” of 170 countries, the way it acquired information without users’ consents made it an ethical conundrum (Narayanan and Zevenbergen, 2015, p. 3). In Narayanan and Zevenbergen’s critique paper, they examined the ethical conundrums Encore project faced based on the “structure and the set of principles used” in the Menlo Report (Narayanan and Zevenbergen, 2015, p. 8).

Narayanan and Zevenbergen provided “an ethical inspection” to start their analysis (Narayanan and Zevenbergen, 2015, p. 8). Firstly, they analyzed who the stakeholders are and reached to the conclusion that “any Internet user worldwide can stumble upon the invisible Encore script and carry out a censorship measurement” (Narayanan and Zevenbergen, 2015, p. 9). They also concluded that “the worldwide scale of Encore” made it infeasible to analyze “all potential stakeholders individually” and it contradicts with “the goal of scalability” (Narayanan and Zevenbergen, 2015, p. 9).

The two authors then explored the question of whether Encore is “human-subjects research” (Narayanan and Zevenbergen, 2015, p. 10). To answer the above question, the question of “whether or not IP addresses constitute personally identifiable information”, has to be answered (Narayanan and Zevenbergen, 2015, p. 10). However, that question is still under debate.

Next, the authors applied the “principal of beneficence” by trying to identify “potential benefits and harms” (Salganik, 2018, p. 302; Narayanan and Zevenbergen, 2015, p. 11). However, Encore’s global scale made it hard to define and identify potential risk and harms (Narayanan and Zevenbergen, 2015, p. 11). In the discussion of benefits, it is clear that “measurement helps illuminate censorship” in terms of “both its motivations and the technologies behind it” (Narayanan and Zevenbergen, 2015, p. 11).

Narayanan and Zevenbergen then discussed whether Encore “presents more than minimal risk” and how to mitigate harm (Narayanan and Zevenbergen, 2015, p. 13). Burnett and Feamster made the claim that “normal web browsing exposes users to the same risks that Encore does” from a “consequentialism” view, however, Narayanan and Zevenbergen reveals several caveats regarding to this argument (Narayanan and Zevenbergen, 2015, p. 13; Salganik, 2018, p. 302). The authors then discussed how mitigating harm could be achieved in terms of “informed consent, transparency and accountability” (Narayanan and Zevenbergen, 2015, p. 14).

In the end, the authors argued that the Encore researchers cannot be sure that their measures didn’t violate any local law.

(b)

My assessment would be based on the four principals proposed in Salganik (2018). Firstly, the Encore project didn’t show respect for persons. Users are not asked for consent when their web browsers are directed to censored websites. Thus, they are not being “treated as autonomous” (Salganik, 2018, p. 305). With regard to Beneficence principal, just as Narayanan and Zevenbergen mentioned, though the benefits are clear, it is hard to identify potential harms (Narayanan and Zevenbergen, 2015). Third, the principal of justice also needs more attention. The Encore project is practiced on a global scale, which meant it involved users under different censorship systems. Thus, it is hard to measure the distribution of potential benefits and risks. Finally, the global feature of the project also brought difficulties to determine if the project complaint with the local law.

References

Barbaro, Michael and Tom Jr. Zeller, “A Face Is Exposed for AOL Searcher No. 4417749,” New York Times, August 9, 2006.

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

Kauffman, Jason, “I am the Principle Investigator...,” Blog Com- ment, 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, MichaelZ- immer.org, http://www.michaelzimmer.org/2008/09/30/ on-the-anonymity-of-the-facebook-dataset/, Sep. 30, 2008c.

Mayer, Jonathan, Patrick Mutchler, and John C. Mitchell, “Evaluating the Privacy Properties of Telephone Metadata,” Proceedings of the National Academy of Sciences of the USA, 2016, 113 (20), 5536–5541.

Montjoye, Yves-Alexandre de, Laura Radaelli, Vivek Kumar Singh, and Alex Sandy Pentland, “Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata,” Science, 2015, 347 (6221), 536–539.

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