<Assignment 8>

Donghyun Kang

1. Identification risk in anonymized data

(a) Pick two of the examples in Table 1 and describe in one or two paragraphs how the re-identication attack in both cases has a similar structure.

I picked up Montjoye et al. (2015) and Zimmer (2010) from Table 1. First, Montjoye et al. (2015) showed that the individuals could be easily re-identified based on the anonymized credit card transactions data in which contained the geographical information of the shops, time, and price. Using simulations with different resolutions for spatial, temporal, and price ranges, the authors found out that "coarsening the data is not enough to protect the privacy of individuals in financial metadata datasets." (Montjoye et al. 2015, p. 538) The analysis of "Tastes, Ties, and Time" (T3) research project by Zimmer (2010) also revealed that anonymized data in a traditional sense could be easily re-identified drawing upon the information in data. The T3 research team collected the profiles of a cohort of Harvard undergraduates (n = 1,640) and linked the Facebook data with the administrative data such as demographics, the name of majors, so and so forth. Despite the difference that Montjoye et al. (2015) 's data had 1.1 million observation points with three columns (location, time, and the price), which I would label "large but shallow data) whereas the T3 team constructed relatively small (n = 1,640) but "deep data," both cases demonstrate that the simple anonymization that hides the personal identification of individuals is not sufficient to safeguard privacy, especially when data sharing is required for the purpose of guaranteeing rigorously scientific research. Plus, the two examples show that abiding by the U.S. standard does not mean that it satisfactorily qualifies the standard of European Union, which has relatively more restrictive.

(b) In one or two paragraphs, describe how the data could reveal sensitive information about the people in the dataset for each of your two examples.

As discussed above, both cases show that data can be utilized to reveal individuals' information for the digital trace can function something similar to "fingerprint." Montjoye et al. (2015) figured out that a few random transactions of individuals drawn from the credit card transaction data were sufficient to trace back the users' ID, with the information of time, price, and the location of shops in terms of unicity measure. This potential of the users' unique transaction patterns is per se quite sensitive topic because people consider this information private matter. For example, "Among Americans, 87% consider credit card data as moderately or extremely private." (Montjoye et al. 2015, p. 537) Moreover, the credit card data can be used for a variety of different purposes such as "credit scoring, fraud detection, and understanding the predictability of shopping patterns." (Montjoye et al. 2015, p. 537)

The dataset employed by the T3 project team show another way that the simply anonymized data could breach privacy. Even though the research proposal passed the Institutional Review Board and the research team did not entirely ignore the potential issues, they failed to protect the subjects' privacy first because the compositional information such as total number of males and females, and the distribution of the number of majors can actually help other people to target the institute (Harvard) and

the unique data such as nationalities and social networks in Facebook can be utilized to re-identify particular subjects. This again not only displays the validity of the fingerprint analogy but the optimistic expectation that simply deleting individual's identifiers is enough to protect privacy is not defensible.

2. Describing ethical thinking

Kauffman argued that, as a group of sociologists, the T3 team attempted to contribute the body of sociological knowledge which would be beneficial for sociology as an academic discipline. This is basically based on the potential benefit that T3 research would bring in. Kauffman (2008b) also said that they did not breach law in a sense that they only utilized the data publicly on Facebook, which implies that one with Facebook account basically could access the subject's public information that they collected. Thus, Kauffman (2008b) argued that the risk of privacy intrusion for their subjects was not different from other users in a sense that any hackers who were able to break in the Facebook server could get the same type of data, which can be translated into the principle of "Justice." Moreover, Kauffman (2008c) claimed that the research team did not have to get the informed consents from the subjects because it was public in nature. In general, I would say that Kauffman's defense on the T3 research is based on consequentialist' logic.

However, I also think Kauffman's argument shows that the two frameworks of consequentialism and deontology can be easily mingled in attempting to defend one's position. For example, while neither anticipating the potential harm that could be caused by publicly sharing the data without technical knowledge, Kauffman (2008b) seems to claim that they did not intend to cause any harm, which follows the deontologist' logic, and they expected some benefits for the research community, which rather follows the consequentialist' logic. (Of course, it seems that people with stricter deontological position would not agree with the second and the third Kaufmann's quotations given that the research subject should be asked they would consent whether their information could be collected whenever it is possible.)

3. Ethics in Encore

(a)

Drawing upon the ethical principles - "respect for persons", "beneficence", "justice - that were first articulated in the Belmont Report (1979) and the Menlo Report (2012), Narayanan & Zevenbergen (2015) provided an analysis on the Encore study conducted by Burnett and Feamster (2015), which attempted to measure the censorship practices across the world. Narayanan and Zevenbergen (2015) first argued that it was hard to identify proper stakeholders in the Encore study because of the scale of the study design. They showed that the general consensus on the importance of scalability among computer scientists renders it difficult to guarantee the principle of respecting persons that requires researchers to identify the participants of a study. This is also linked with the point that it is debatable whether collecting individual's IP information is equal to conducting research on human subjects.

The authors then applied the principle of Beneficence to the Encore case considering again the global scale of the study. This was because the scalability made it hard to measure the potential harms that the participants would be given, resulting from the complexity of historical and political environments in which they were situated. Narayanan and Zevebergen (2015) suggested the two benefits of Internet censorship research. On the one hand, Encore could help to safeguard the basic human rights related to a free speech given that "illuminating censorship techniques enhances the ability to create effective censorship circumvention tools." On the other, Internet censorship research would be beneficial because the censorship on the internet undermines the "end-to-end" principle, which basically has been underpinning the Internet technology in terms of security and connectivity. As for the costs or potential harms that this type of research might produce, cover one important risk-taking of users: Encore might put internet browser users in unexpected risk of persecution from governments that set up the Internet censorship. Even though Burnett and Feamster (2015) asserted that normal Internet browsing involves the same level of risk as what Encore does, Narayanan and Zevenbergen (2015) argued that what Encore did not meet the user's general expectation about what Internet browsers do, the degree of persecution would vary along the types of websites, and there might be harms with consequences beyond individual persecutions such as a country-level Internet shutdown.

Note that Salganik (2018) summarized that "one of the most fundamental tensions in research ethics" is "using potentially unethical means to achieve ethical ends." (Salganik 2018, p. 302) We can basically see that the framework of consequentialism, which is closely linked to the principle of Beneficence, was employed by Burnett & Zevenbergen (2015) to justify their research while Narayanan & Zevenbergen (2015) pointed out that Burnett & Zevenbergen's consideration regarding the potential harms was not sufficient. In addition to the principle of Beneficence, Narayanan & Zevenbergen (2015) examined the principles of "Respect for Persons" and "Law and the public interest" focusing on "informed consent", "transparency", "accountability." Together with the previous discussion about the principle of Beneficence, Narayanna & Zevenbergen's (2015) explained that the Encore study could have or should have been more cautious, following either the consequentialist or the deontologist framework, saying that "[T]he researchers must then demonstrate that they accept responsibility for their actions and the consequences, and have necessary strategies in place."

(b) In one or two paragraphs, write your assessment of the ethical quality of the Burnett and Feamster (2015) Encore study.

As discussed by Narayanan & Zevenbergen (2015), the Encore case poses a lot of interesting and important ethical conundrums for the computational research community and I would like to first emphasize that Burnett and Feamster should not be considered as evil despite their naivety. This is not only because Burnett and Feamster wanted to achieve something beyond publishing their research - at least indirectly contributed to reveal the nature of the internet censorship and thereby boost the freedom of speech - but also because that the government that would implement the censorship and punish their people who attempt to access a website to get information should be first blamed. This is not an attempt to defense Burnett and Feamster blindly but we still have to note that it is a common sense that a moral objection against any action is truly meaningful when the intention, the action, and

consequence are aligned. Especially given that the costs and benefits are hard to calculate due to the scalability of a research project, I think it might be neither realistic nor desirable for researchers to think about every single possible case in advance. However, this does not mean that Burnett and Feamster did the right things in terms of considering ethical concerns that their research design might raise. For example, I think the fact that they did not get informed consents from the participants actually is quite problematic because it breaches the basic right of being able to have a choice.