Assignment #8

Sanittawan Nikki Tan

12/1/2018

Part 1

I chose to compare Sweeney (2002) and Zimmer (2010).

(a)

Both Sweeney's and Zimmer's articles describe the structure of re-identification attack similarly. In both cases, the general structure is to (i) look within the released dataset and find unique characteristics that could be used to identify individuals (ii) Use another dataset which could be obtained publicly or from proprietary sources that have some common identifiers with the first dataset (iii) use information from both dataset to narrow down to a specific individual. Zimmer describes the process of re-identifying individuals in the released Tastes, Ties, and Time ("T3") dataset as follows. Firstly, some researchers used freely available codebook that the T3 research team provided to narrow down from more than 2000 possible schools to Harvard College by using information of unique names of majors offered at the school in the dataset (Zimmer 2010, 316). Secondly, the re-identification attack on individuals can be done by cross-referencing the individuals in the dataset with publicly available datasets and news media articles. This process can be done much more easily because the T3 researchers disclosed that the data was collected from the students of the class of 2019 from Harvard College. Additionally, in some cases, there is only one individual in the dataset that comes from a unique state or a country; for instance, there is only one student from Delaware and one student who identified himself/herself an Albanian (Zimmer 2010, 319). If that student from Delaware graduated from a high school in Delaware where there was only one student who attended Harvard College in 2006 and if the school were to publish a yearbook online, it is possible for an attacker to use the information from the publicly available yearbook to successfully re-identify that particular student in the dataset, thus thwarting the T3 researchers' attempt to anonymize the data.

Similarly, Sweeney (2002, 558-559) described how she managed to re-identify William Weld, a former Massachusetts governor, by using medical records collected and made available to researchers by the Group Insurance Commission ("GIC") and voter registration records for Cambridge, Massachusetts that she personally purchased for 20 dollars. Because she noticed that although the GIC dataset does not contain names of individuals, both datasets share three common identifiers which are 5-digit ZIP codes, birth date, and sex. Sweeney first narrowed down potential candidates in the voter registration records by birth date and found that there are six people in the GIC dataset that share that birth date. Next, she narrowed the candidates down by sex: among six people, only three were men in the GIC dataset. Finally, Sweeney found that there is only one person in the GIC dataset that has the same ZIP code as governor Weld (Sweeney 2001, 559). Thus, Sweeney was able to re-identify William Weld through these steps. Sweeney's article is particularly interesting and beneficial for researchers who wish to make their data public because not only did she demonstrate how to re-identify individuals based on dataset that was supposed to be anonymous, but she also proposed a technique called "k-Anonymity" which anonymizes the data by ensuring that information for an individual person in the dataset is not distinguishable from at least k-1 individuals in the same dataset (Sweeney 2002, 557-563).

(b)

Re-identification attacks can be harmful in many ways and the data can be used against individuals and their networks who were re-identified in a malicious manner. In the T3 study case, the dataset included a student's home state, political views, sexual interests, gender, ethnicity, and his/her network (Zimmer 2010, 321). An individual who wishes to keep his/her sexual interests and political views secret may be at risk of other exposing their private lives, which could backfire their career or relationship with his/her family. In addition, because the study is about understanding how a network of friends developed, individuals who were successfully re-identified also put their networks of friends at risk as well. In the GIC case, medical

records are considered extremely sensitive because it can affect individuals' career or put them at risk of companies that prey on people with a certain illness. For example, if the information of successfully linked individuals in the GIC dataset were to be sold to a pharmaceutical company or a marketing company that sells certain drugs, the individuals may be contacted unwillingly. In another scenario, a job candidate with certain diseases may be discriminated against by employers if the employers were to have access to their private medical records without that candidate's consent. Therefore, re-identification attack that reveals sensitive data could bring about countless negative consequences on individuals.

Part 2

Please note that I took into account the full version of Kaufman's comments on Zimmer's website when rewriting Kaufman's comments.

Kaufman's original comment	**Rewritten comment**
"We're sociologists, not technologists, so a lot of this is new to us ... Sociologists generally want to know as much as possible about research subjects."	"We're a team of sociologists and we acknowledged that we did not sufficiently seek advice from privacy experts before releasing the data. However, we did think long and hard about the cost/risk and benefit of releasing it to the academic community. In sociological research, it is often beneficial for other researchers who wish to build off of our study to know as much as possible about research subjects. We came to the conclusion that the benefits outweigh the cost, and the risk associated with the released of the data can be minimized with proper measures. That's why we ensured that the data that we released cannot be linked to the individuals although you have found loopholes in our methodology. With the effort that we put in to anonymize data, we thought that it was sufficient and revealing information about individual preferences was fairly safe. Moreover, not only did we consider the benefits to the scientific community, but we also care about the reproducibility and transparency. That also plays a part in our decision to publish the data. Don't you think that the release of data can be justified based on these reasons?"
"What might hackers want to do with this information, assuming they could crack the data and 'see' these peoples Facebook info? Couldn't they do this just as easily via Facebook itself? Our dataset contains almost no information that isn't on Facebook. (Privacy filters obviously aren't much of an obstacle to those who want to get around them.)"	"The data that we used is already public on Facebook. Hackers can see the same information that we do. Because we used only data that the owner of the Facebook profile wants the public to see, we actually respected the privacy of the owners by not attempting to find information that the Facebook owner does not want the public to see. In this light, we do not see any reason why additional consent should be sought from individuals either because those individuals have already agreed to Facebook's terms of service and are willing to let others see their profiles. The owners should already be aware of the fact that any information out there is a fair game for anybody and researchers to use it for observational studies."

Kaufman's original comment	Rewritten comment
"We have not accessed any information not otherwise available on Facebook. We have not interviewed anyone, nor asked them for any information, nor made information about them public (unless, as you all point out, someone goes to the extreme effort of cracking our dataset, which we hope it will be hard to do)."	"We are aware of the principle of respect for law and public interests. We sought agreement with Facebook before conducting studies. We complied with that agreement by not using the information we obtained for other purposes than academic. Plus, our project was approved by our IRB. We are very clear and transparent about our methods by making the codebook and data available so that other researchers can cross-check our study. Again, we thought that we have made it extremely difficult for anyone trying to crack our dataset before releasing it. Still, I personally believe that because we did not violate any laws and have carefully considered risk and anticipated benefits, it is in the best interests of everyone that we made the data available although there are some minimal risks to individuals in the dataset."

Although I attempted to rewrite Kaufman's comments taking into account consequentialist ethical framework as well as ethical principles, namely respect for persons, beneficence, and respect for law and public interest, I believe that Kaufman and his team's attempt to anonymize the data and explanation cannot be justified. Firstly, Zimmer (2010, 318, 322) was right to point out that the T3 researchers actually used undergraduate research assistants who were in the school's network to obtain data which may not be publicly viewable to people who are out of the network due to Facebook privacy settings. In this sense, the research team seems to circumvent – or violate – the principle of respect for persons because some profile owners intend for only people in the network to know about their preferences, not the general public when the researchers released the data. Secondly, I think that the T3 researchers did not satisfy the justice principle because it is clear that the students whose data was published bear the most cost while it is true that the research may have created some benefits. To me, it is questionable if the benefit from this study really exceeds the risk of sensitive information being revealed. Additionally, even though the benefits can be argued to exceed the cost/risk from the society perspective, it creates a dilemma if the study creates any benefits for people in the study at all. Thus, applying consequentialist approach on both the society and individual sides still yields ambiguous conclusion, let alone deontologist framework which will argue that this study is unethical based solely on data collection methods (Salganik 2018, 302).

Part 3

(a)

In *No Encore for Encore? Ethical questions for web-based censorship measurement*, Narayanan and Zevenbergen (2015, 1) assessed and analyzed ethical issues of the Encore project, which was carried out by Sam Burnett and Nick Feamster, through established ethical principles and standard outlined in the Belmont and Menlo reports.

The authors began by briefly surveying methods used in computer science research which could be categorized as intrusive methods and non-intrusive methods. Encore project is classified as adopting the intrusive method (4). Narayanan and Zevenbergen also briefly discussed the nature of computer science research and ethical gatekeeping which is significantly different from social science research as well as research in other disciplines that regularly involve human subjects. In the computer science field, research review often occurs after the research is complete. Program committee members include mostly domain experts and are formed and disbanded after each conference. As a result, ethical oversight in computer science research is less consistent (Narayanan and Zevenbergen 2015, 6-7). After having established sufficient background, the authors proceeded to analyze the ethical quality of the Encore research project on the following four issues.

Firstly, Narayanan and Zevenbergen found that their attempt to analyze all stakeholders involving the research project revealed conflicts between scalability, which is a key concept in computer science and engineering, and the idea of minimizing the number of research subjects in fields that conduct human-subject experiments. This conflict leads to another key and controversial question of whether or not Encore is a human-subject research (9-10). Although Burnett and Feamster mentioned in their paper that Georgia Tech Internal Review Board (IRB) did not classify Encore as a human-subject research (2015, 664), it seems that this is an open question from Narayanan and Zevenbergen's perspectives because the debate of "human-subject research" is ongoing and its definition is evolving.

Secondly, the authors expressed concerns on Encore with regard to the principle of beneficence. Narayanan and Zevenbergen noted that although Burnett and Feamster argued that the risk that Encore exposed to users are no more than what users face in normal web surfing, researchers need not engage in "ethical race to the bottom" and should be subject to a higher ethical standard than that of marketing and other players on the Internet (13). Additionally, the authors also noted that the magnitude of harm to users whose computers were used to access censored websites depends largely on the type of censored website and laws across different countries (13). Nevertheless, the authors acknowledged that Encore study presents various benefits on internet censorship which could provide a greater understanding of censorship mechanisms and creative ways to combat them (11). Thus, the authors appear to conclude the Encore study satisfies the beneficence principle and that the risks can be mitigated. Applying the consequentialist framework here would also lead to the conclusion that the goal and the anticipated benefit should justify the study.

Thirdly, the authors found that Encore researchers should seek informed consent from users or make the information on Encore more obvious on volunteer websites. Narayanan and Zevenbergen argued that although Burnett and Feamster's arguments against seeking informed consent, in this case, are valid, the researchers should still consider the possibility that users in oppressive regimes may face unfair trials and plausible deniability may be insufficient to protect a user.

Lastly, Narayanan and Zevenbergen concluded that Encore study did not violate any U.S. laws, especially its compliance with United States computer law (15). However, they also noted that jurisdiction is unclear in many cases since Internet users participating in this project could be from anywhere.

(b)

The Encore study by Burnett and Feamster presents a creative way to measure censorship; however, it also poses several ethical challenges that future researchers should consider. The study's ethical quality can be assessed based on four principles as outlined by Salganik (2018, 294-301). Firstly, whether or not the Encore study complies with the principle of respect for persons is questionable. Burnett and Feamster maintained that informed consent should not be sought from participants in their research because of difficulties in communicating technical concepts and the risk to participants if there are any traces from informed consent (Burnett and Feamster 2015, 664). It is true, as Burnett and Feamster put it, that researchers should focus on minimizing the risk and protect uninformed users. However, I still agree with Narayanan and Zevenbergen (2015, 15-16) that there should be more obvious information about whether a user's computer participated in the research project. Secondly, in terms of the principle of beneficence, I think that Burnett and Feamster put a lot of effort into minimizing the risks to users. However, because this project can have serious consequences on users who live in oppressive regimes with censorship without their knowing, the researchers should have limited the number of websites per users or diversified the type of risky websites that a computer can send an access request. Because the Encore project has clear benefits to enriching our knowledge on censorship and the risk to users can be mitigated, I think that the Encore project satisfies the principle of beneficence.

Thirdly, the principle of justice concerns whether the risks and benefits of a research project are proportionately and moderately distributed among research subjects and those who benefit from the study. In the case of Encore, I think it is questionable if the study satisfies this principle. On the one hand, there are a large number of participants spreading across the world due to the scalability of the project. In addition, it is unclear which jurisdiction the study and action of individual computers are subject to and the laws differ across the jurisdiction. So, it is quite difficult for governments to keep track of all the participants in the study. On the other hand, it is also possible that if there are only a few users from a country and the government was able to track all of them. The costs of these participants would be very high because it could mean

that some users and their families may have to flee the country or face unfair trials in their home country. Ideally, if the participants of this research were to grant consent and understand the risks associated with the study, it would be easier to assess if Encore satisfies the justice principle. Finally, as Narayanan and Zevenbergen pointed out that the Encore study did not violate any U.S. laws, it is clear that Encore satisfies the compliance part of the principle of respect for law and public interest. However, Salganik mentioned that there is also the transparency-based accountability part of the principle that has yet to be assessed. Having read Burnett and Feamster's research paper, I think that both researchers satisfied the accountability part of the principle because they have openly discussed their research goals, methods, and ethical issues in their paper. The paper was published in the SIGCOMM Conference paper. It appears that both authors realized the ethical concerns of their project and outlined steps that they sought as shown in table 2 (Burnett and Feamster 2015, 664). Thus, I think that the Encore project satisfies the final principle. In summary, although it is questionable if the project satisfies the principle of respect for persons and justice, the authors adequately addressed and complied with the principle of beneficence and respect for laws and public interest.

Burnett, Sam, and Nick Feamster. 2015. "Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests." In Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, 653–67. SIGCOMM '15. London: ACM. https://doi.org/10.1145/2785956.2787485.

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

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. 2010. "But the Data Is Already Public: On the Ethics of Research in Facebook." Ethics and Information Technology 12 (4):313–25. https://doi.org/10.1007/s10676-010-9227-5.