Assignment #8
MACS 30000
Delores Tang
12.1

1. (a) The two examples I pick are Health Insurance records in Sweeney (2002) and Mayer et al. (2016). Both articles closely illustrate how re-identification through linking will cause informational risk and, in turn, harm the effectiveness of "anonymization" of data as mentioned in Salganik (2018, Ch 6.6.2) Re-identification attack is the process of which researchers merge two sources of data that, individually, are safe and anonymous, one with potentially sensitive information, and another with identification information, to be able to link subjects' private information to their identities, which causes informational risks (Salganik, 2018, Ch 6.6.2).

   Therefore, both studies are similar in ways they used two data sources, one with Personally identifiable information (PII; Salganik, 2018, Ch 6.6.2; Mayer et al., 2016, p. 5538) and another is non-PPI (p.5538) but with sensitive information about subjects of data to combine together to re-identify individuals who are subjects of data. In Sweeney (2002, p.2), the PPI data was medical records while the non-PPI was voting records (PII; Salganik, 2018, Ch 6.6.2). Researchers matched two data sources' overlapping attributes, ZIP code, Birth data and Sex, and successfully re-identified subjects of the data. In Mayer et al. (2016), the non-PPI data was people's telephone numbers while the PPI data was information they inputted in social network application programming interfaces (APIs; Mayer et al., 2016, p.5538). Some shared attributes included location and relationship (p.5539) and were used in re-identification.

   (b) In Sweeney (2002, p.2), researchers combined two data sources: the Group Insurance Commission (GIC) data that contains individuals' medical records including individuals' Ethnicity, Visit date, Diagnosis, Procedure, and Medication (p.3) but not specific PPI attributes, and a purchased voter registration list including Name, Home address, Party affiliation, and Date registered as voters (p,3) for Cambridge Massachusetts (Sweeney, 2002, p.2) that includes PII (Salganik, 2018, Ch 6.6.2). By matching the two data sources' shared attributes including Zip Code, Sex, and Birth Date, Sweeney (2002, p.3, Figure. 1) was able to identify individuals' identity (such as name and address). Similarly, Mayer et al. (2016) researchers used data from an Android smartphone application that collects users' call and text data (p.5536) and social network application programming interfaces including user information in applications such as Facebook, Yelp, and Google Places (APIs; p. 5538). By matching non-PII and PII (Salganik, 2018, Ch 6.6.2) such as location and addresses inputted in Facebook and Yelp, relationship

information from call and text message logs, and other sensitive information (p. 5539-5540), researchers were able to successfully re-identify their subjects.

2. A common mistake that sociological researchers sometimes make is that they fail to strike a balance between the two ethical frameworks mentioned in Salganik (2018, Ch 6.5): the consequentialism and deontology. Jason Kaufman (Sep. 30, 2008a), though partially acknowledged the harm their research might cause to Harvard college students, still emphasized the value of it - "they do indeed have the potential to compromise subjects, though they will be enormously useful to researchers interested in taste, culture, etc". He potentially attempted to justify the reason for using and making public of the data because "sociologists generally want to know as much as possible about research subjects" (Sep.30, 2008a). However, the scientific significance of research questions does not necessarily give permission to researchers to explore them using ethically controversial methodologies because "use potentially unethical means to achieve ethical ends" (Salganik, 2018, ch 6.5) - sacrificing deontology in order to emphasize consequentialist values - violates research ethics.

In addition, what Kaufman and his colleagues have attempted to do violated the "Respect for Persons" principle listed in Salganik (2018, ch. 6.4.1), which suggests that participants' autonomy should be protected by asking for their informed consents. Kaufman argued in his comments that difficulties could arise when asking for consents - "On the issue of the ethics of this kind of research - Would you require that someone sitting in a public square, observing individuals and taking notes on their behavior, would have to ask those individuals' consent in advance?" (Sep. 30, 2008b). Nonetheless, Kaufman's study is essentially different in objectives and nature from natural observations of people's behaviors. Their data includes specific, sensitive, and private information about their subjects including gender, ethnicity, home state, political views, major/minor, and cultural backgrounds (Zimmer, Oct. 3, 2008b). In this specific case, their participants' anonymity could not be promised, and whether they would like to disclose that information to the public was unknown.

3. Narayanan and Zevenbergen (2015) analyzed the Encore web censorship project (Burnett & Feamster, 2015) using frameworks, "respect for others," "beneficence" and "justice", as principles mentioned in Belmont Report (Narayanan & Zevenbergen, 2015, p.8) and Salganik (2018, Ch 6). The article firstly introduces the Encore project, which is a web censorship study that invites web administrators to copy-paste a snippet into the source code of the page that would direct visitors' browser to access potentially filtered websites surreptitiously (Narayanan & Zevenbergen, 2015, p.2). Through this process, researchers were able to conduct censorship measurement to collect data about censorships in different places of the world.

Narayanan and Zevenbergen (2015, p.3-7) then outlined the technical and ethnic backgrounds of censorship measurement studies, especially those also utilized similar

methodologies. Studies like Encore project usually have the research objective to understand what content, when, where, and how censorship operates (2015, p.5). They, at the same time, always face similar methodological difficulties, such as personal information leakage and legal disputes as well as proposing potential risks to subjects (p.6), and also has ethical problems such as the lack of a scholarly ethics expertise in the committee (p.7).

Analyzed by Narayanan and Zevenbergen (2015, p.9), first and foremost, the Encore project, in specific, is a human-subject study because it has collected personally identifiable information from human subjects and should comply to human-subject research ethical standards before being conducted publically. Second, according to their beneficence analysis of the study, this project has positive benefits because censorship itself poses threats to the principle of justice (Narayanan & Zevenbergen, 2015, p.12; Salganik, 2018, ch 6.4.3). But it, as well, has potential harms because accessing to users' personal devices and information essentially puts them in risks especially in nations where a break of censorship regulations could cause serious consequences to individuals (p. 13) and is usually against users' wills. Such risks could be mitigated if researchers could ask for individuals' informed consent and, thus, ensure the transparency and accountability of the project. Last but not least, because Encore is an international project, it could violate regulations in certain nations and legal compliance issues (p.16).

Throughout the analysis, one important framework Narayanan and Zevenbergen (2015, p.11-15) has referred to is the beneficence analysis and its basis in the principle of beneficence (Salganik, 2018, ch 6.4.2; ch 6.5). As mentioned earlier, the study's benefits are mainly based on the uniform belief that censorship violates human rights (p.13). According to the framework of consequentialism, Encore has good research intent despite its flawed means (Salganik, 2018, ch 6.5). Extreme consequentialists would argue that it conforms to the principle of beneficence, and its methodologies should not be a matter of concern. However, from a deontology point of view, Encore violates the first principle by failing to respect their participants' autonomy and, thus, should be questioned on the basis of its research methods (ch 6.5). Researchers should aim to strike a balance between the two frameworks - the consequentialism and the deontology (ch 6.5), and it is usually done by asking for the informed consent from participants. Informing participants about potential risks and harms of the study and only include those who consent to participate would allow researchers to comply with deontologists' view of methodological ethics while being able to achieve a significant end according to the consequentialism.

(b) Different from Narayanan and Zevenbergen (2015), I would like to analyze the Encore project (Burnett & Feamster, 2015) from another perspective of the principle of justice as mentioned in Salganik (2018, ch 6.4.3). The principle of justice essentially addresses the problem of distribution of harms and benefits across research subjects (ch 6.4.3). Two important elements of this principle include protection (protecting the vulnerable) and access (giving equal opportunities to access beneficial resources given by the study; Salganik, 2018, ch 6.4.3). A

study that violates this principle might have an unequal distribution of benefits and harms over different social groups, or its benefits could not be accessed by certain groups of individuals.

One harm of the Encore web censorship project (Burnett & Feamster, 2015) is that researchers failed to protect participants' autonomy and their private information (as elaborated in both Salganik, 2018, ch 6.2.3 and Narayanan & Zevenbergen, 2015). Moreover, certain participants seemed to be more vulnerable to those harms brought by this project. Specifically, individuals' devices could be more vulnerable than organizations' and institutions' devices that are usually equipped with more advanced firewall and security softwares and contain less personally identifiable information. Thus, I argue that Encore fails to distribute its harm equally to all of its potentially interested population.

In addition, participants in the Encore project are not homogeneous in terms of their nationalities and their use of devices and, therefore, could be influenced by this project differently. Most importantly, it is unclear that whether participants of the study could be those who are benefited by it. Burnett and Feamster (2015)'s research has participants in countries such as Egypt, South Korea, Iran, Pakistan, Turkey, and Saudi Arabia (Narayanan & Zevenbergen, 2015, p.3), some of those have strict media and web censorship, and violating legal regulations related to censorship could be regarded as violations of law. Thus, nations being measured in Encore might be those that are most unlikely to change their censorship regulations. As a result, even if the beneficence analysis suggests that the Encore project brings benefits to the society, it is unlikely to be the society where most of Encore's participants reside in. Thus, not all participants could have access to benefits of the Encore project, and Encore essentially fails to comply with both the protection and access elements of the principle of justice (Salganik, 2018, ch 6.4.3).