Question 1

As described in Salganik (2018), although researchers ensure that data sets containing sensitive information remain anonymous, these datasets can still be combined with other datasets or other unique information about the data, to identify specific individuals or groups, therefore compromising their privacy. For example, by combining the voting records of residents in Cambridge, Massachusetts with anonymized health records of state employees released by the Group Insurance Commission (GIC), one can deduce which medical records belongs to which individual. Specifically, as both datasets share the same fields of zip code, birthday and sex, Sweeney (2002) showed that by combining these three types of information, one can identify match individuals to their medical information, even identifying William Weld's (the 68th governor of Massachuetts) medical records. Similarly, in another example of a re-identification attack, Zimmer (2010) notes that by looking at the anonymized dataset from the project, *Tastes, Ties and Time,* and other public comments, one can identify that the individuals analyzed in the study were students of Harvard College. To elaborate, Zimmer (2010) describes how the anonymous dataset revealed unique information about the college the researchers studied- the school is private, co-ed and the freshman class had 1640 individuals. With the information that the school is in New England, and as Harvard College is the only institution that allows students to take certain unique majors that are denoted in the dataset, it was definitive that the individuals in the dataset were from Harvard College.

The above examples illustrate that even though the original datasets remained anonymous, sensitive information about individuals can be easily revealed to the public. Specifically, based on the method described by Sweeney (2002), sensitive medical information containing records of 'diagnosis, procedures, and medications' (Sweeney 2002, 3) can now be linked and identified to every specific individual coded in the GIC dataset. If this information is publicly available, companies promoting fraudulent medical practices may even use this data to target advertisements to specific individuals with medical conditions and influence their drug purchases. Additionally, discrimination may happen as a result – if data of those who have stigmatized illnesses such as sexually transmitted diseases and mental illnesses are made available, those who have these illnesses may experience discrimination from others in their career and personal relationships.

Additionally, although Zimmer (2010) also notes that although 'individual subjects were not identified in the process' (Zimmer 2010, 317), the dataset still revealed that individuals' housing records and gender, race, home state, political views, sexual interests and college major (Zimmer 2010, 321), can now be easily matched to specific individuals in Harvard College. In this case, students who are in the midst of negotiating with their sexual or gender identities, like those who identify as LGBTQ, may also feel very uncomfortable having this information online. They may also experience discrimination, especially from more socially conservative individuals around them.

Question 2

From Kaufman's comments, it seems that he is defending himself by using the consequentialism framework. Specifically, he argues for the benefits of compiling this dataset- that as 'enormously useful to researchers interested in taste, culture, etc' (Kaufman 2008b), compiling this dataset can be considered the type of research that sociologists should pursue. By using this Facebook data coupled with housing records, he and his other researchers emphasize that they are now able to build and analyze a 'complete social universe' (Kaufman 2008a), that was previously unprecedented in past research looking at social networks, suggesting that this data is and will be very beneficial in furthering sociological research on human behavior. On the other hand, Kaufman also argues that as 'our dataset contains almost no information that isn't on Facebook' (Kaufman 2008c), the risks of individuals using Facebook normally should be the same as the risks of

publishing this dataset publicly. Kaufman has also taken action in mitigating the risks of identifying personal information of these students, suggesting the use of principle, Beneficence- the researchers did not seek out additional information from the students ('we have not interviewed anyone, nor asked them for any information nor made information about them public' (Kaufman 2008c)), therefore ensuring that no unique information of the students is readily and publicly available. They also anonymized the data to mitigate the risk of readily revealing sensitive information of the individuals. Following his argument then, he and his team of researchers seem to have considered the risks and benefits of compiling this data, and ultimately decided that the benefits of such research far outweigh the risks faced by these individuals. Although one can argue that he and his team have underestimated the risk of publishing this information and did not fully take the time to mitigate the possibility of the revelation of sensitive information, as it took just a matter of days before it was identified that the data was from Harvard College, he also expressed that he is 'not technologists, so a lot of this is new to us' (Kaufman 2008c), implying that he did not have the skills to fully comprehend the ease in which the dataset could be compromised.

However, by adopting a deontologist standpoint and by considering the principles of Respect for Persons, Justice and Respect for Law and Public Interest, one can argue that he and his researchers should have given more thought before pursuing this research. Based on the principle of Respect for Persons, which Salganik (2018, 295) notes is closely in line with deontological thinking, even if Kaufman and his team believed that the study is of low risk to individuals and may even be beneficial in the long run (for example, if the study reveals critical information about social networks that can be used to policy research), one must still consider that these Facebook users in the study did not give explicit consent to participate in their research. To elaborate, providing information online about oneself does not mean that one consents to the collection of this data, that is, we cannot assume that Facebook users would reasonably foresee (and also accept) that their information will be collected and analyzed by researchers when they use their Facebook account. This suggests that Kaufman and his team did not consider the autonomy of these Facebook users, suggesting that they have failed to adhere to this principle.

Additionally, according to the principle of Justice, one group 'should not bear the cost of research while the other group benefits' (Salganik 2018, 298). In this case, as the Facebook users in the study were not randomly selected (as they were all Harvard college students), and were not compensated for the risks of participating in this data, those in the dataset bore the cost of research compared to the public who benefitted from the research. Thus, we can argue that Kaufman did not consider this principle in implementing this study.

Lastly, for the principle of Respect for Law and Public Interest, Kaufman and his team did get consent from Harvard IRB, Facebook, and Harvard itself. However, as argued by Zimmer (2010, 318), Kaufman and his team did not consider that as those who were manually scraping the data (i.e. research assistants) were from Harvard, they might have access to Facebook data that is not publicly available, and is only available to those who are the Harvard network. In this case, even though Kaufman and his team did obtain consent from Facebook, did they consider how Facebook's terms and conditions may be violated in this regard? Considerations for this principle thus should have been expressed in their research.

Based on the above arguments, I believe Kaufman and his team should have more thoroughly investigated these considerations, or at least pondered about the ethical concerns of this project before pursuing this research. Although Kaufman and his team have arguably acted 'in good faith' (Zimmer 2010, 323) at that time, with their own cost/benefit analysis of their research, they should have deliberated the ethical concerns more comprehensively by analyzing their own research using these principles and considering the deontological framework.

Question 3

In Narayanan and Zevenbergen (2015)'s *No Encore for Encore? Ethical Questions for Web-Based Censorship Measurement,* they describe the ethical concerns of Burnett and Feamster (2015)'s *Encore* study. Specifically, using the guidelines of the Menlo Report, they first discuss the difficulty of identifying the stakeholders in the study, then apply the principle of Beneficence and a consequentialist framework and lastly, discuss the principles of the respect for persons, law and public interest as reflected in the study.

Firstly, in their discussion about the ethical quality of the *Encore* study, they note the difficulties in identifying the stakeholders of the *Encore* study - not only is looking at all stakeholders in the study individually unfeasible, there remains much debate if *Encore* should be deemed as human-subjects research. Specifically, although Princeton and Georgia Tech IRB do not deem the study as a human-subjects study (Narayanan and Zevenbergen 2015, 9), Garfinkel argues that 'computer security research should be viewed as human-subjects research (Narayanan and Zevenbergen 2015, 10), illustrating the difficulty in applying a universal ethical framework to the research.

Secondly, they also apply the principle of Beneficence and use a consequentialist framework to examine the ethical concerns of the *Encore* study. As described by Salganik (2018, 295), Beneficence is 'deeply rooted in consequentialist thinking'. As such, Narayanan and Zevenbergen (2015) first identify the benefits of the *Encore* study using a consequentialism framework – that the results of the study help to better understand the phenomenon of censorship, as censorship is perceived to be harmful to the citizens of the state. That being said, they also note that 'an unequivocally negative view of censorship is not universally held' and the results of such studies may also be difficult to interpret (Narayanan and Zevenbergen, 2015, 12). In terms of the risks, although Burnett and Feamster argue that 'normal web browsing exposes users to the same risks that *Encore* does' (Narayanan and Zevenbergen, 2015, 13), Narayanan and Zevenbergen still suggest that they could have been more thorough in analyzing the risks of the study. Specifically, they argue that Burnett and Feamster have failed to consider that online users do not reasonably expect to participate in online tracking practices and that users who unwittingly participated in the Encore study may also have a higher likelihood of state persecution, although this is dependent on which censored website accessed and the country legislation of the user (Narayanan and Zevenbergen 2015, 13). Additionally, they argue that another type of risk that the researchers failed to consider is that the state shuts down the Internet in which the user is from (Narayanan and Zevenbergen 2015, 14). They also acknowledge how the *Encore* researchers have sought to mitigate the risks, but still note that they could have gone further in consulting as many academics as possible in analyzing the ethical quality of the project.

Lastly, Narayanan and Zevenbergen also apply the principles of Respect for Persons, Law and the Public Interest. They propose that although ideally, obtaining informed consent from those participating in the *Encore* study is ideal, Burnett and Feamster argue that it remains unfeasible and chose to provide a statement at the bottom of the website explaining the possible legal consequences for users in the study instead. Narayanan and Zevenbergen also note that the *Encore* researchers cannot be certain if their users have violated any laws as users are from all over the world (Narayanan and Zevenbergen 2015, 15-16).

I believe that Burnett and Feamster should have done more in ensuring that the study can be considered ethical. Although censorship research is certainly useful, even if this phenomenon is not universally acknowledged as harmful for individuals, the *Encore* researchers should have more thoroughly deliberated the ethical concerns of the study. Firstly, although they have considered obtaining informed consent from individuals and have concluded that it remains unfeasible, they still could have gone further in providing more information to users and placing the opt-out link more

prominently, as argued by Narayanan and Zevenbergen seen above (2015, 15). This suggests that the Encore researchers could have done much more to adhere to the principle of the Respect of Persons. Additionally, although they calculated the risks and benefits of the research and chose to pursue this study because the benefits outweighed the costs, I believe they have not considered the high risk of persecution that some individuals from certain countries with tight censorship controls may bear. For example, if the user is from China, if the government determines that they have sought to access banned websites that contain extremely sensitive political information, the consequences for this individual may be severe and even result in imprisonment. This relates to the principle of Justice- some individuals from particular countries will disproportionately bear most of the cost of this study, while others reap the benefits. Although as noted above, the researchers have sought to mitigate the risks by testing only social media websites in the current version of Encore (Narayanan and Zevenbergen 2015, 14), they not only should have done so earlier, but they could have also considered excluding individuals from countries with oppressive censorship controls to mitigate the risks of the study. Lastly, although Burnett and Feamster have ensured that their research process is transparent and accountable as their results are published in an academic journal, whether they have satisfied the compliance component of the principle of Respect for Laws and Private Interest, remains circumspect- as also discussed above, the censorship, privacy and data laws of many countries also differ widely and it remains unclear if the Encore researchers have violated this aspect (Narayanan and Zevenbergen 2015, 15-16). In this case, although the benefits of this research remain very high, I believe that the Encore researchers should have done more, or at least actively considered more of these ethical concerns when implementing their study.

References

Kaufman, J. (2008a). Considering the sociology of Facebook: Harvard Research on Collegiate Social Networking [Video].: Berkman Center for Internet & Society.

Kaufman, J. (2008b). I am the Principal Investigator… [Blog comment*]. On the ''Anonymity'' of the Facebook dataset* Retrieved September 30, 2008, from http://michaelzimmer.org/2008/09/30/on-the-anonymity-of-the-facebook-dataset/.

Kaufman, J. (2008c). Michael—We did not consult… [Blog comment]. *michaelzimmer.org* Retrieved September 30, 2008, from http://michaelzimmer.org/2008/09/30/on-the-anonymity-of-thefacebook-dataset/.

Salganik, M. (2018). *Bit by Bit: Social Research in the Digital Age*. Princeton University.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty Fuzziness and Knowledge-Based Systems*, 10(5), 557–570.

Narayanan, A. and Bendert Z. (2015), "No Encore for Encore? Ethical Questions for Web-based Censorship Measurement," *Technology Science*.

Zimmer, M. (2010). "But the Data is Already Public: On the Ethics of Research in Facebook." *Ethics and Information Technology*, 12(4), 313-25.