Question 1. Identification risk in anonymized data.

Part a.

"Health insurance records" (Sweeney, 2002) and "Demographic, administrative, and social data about students" (Zimmer, 2010) datasets, are an example of a dataset that has the same re-identification attack structure. The data available to public without any personal level details such as, names of individuals, address locations and telephone numbers, are often merged with other datasets, based on the characteristics common to both the datasets. Eventually, using the merged dataset, re-identifying the individuals becomes possible. For example, upon merging "Health insurance records" data with voting records of Cambridge city, one can obtain medical records of a person with a given birth date and a zip code in Cambridge city.

"Demographic, administrative, and social data about students" dataset had information about friendship network, cultural tastes of the incoming freshmen at a private college, along with their academic majors and information about their residence on campus. The description of college in the data made available to public was matched with search results obtained through "College Board" online database. After performing the search, the number of potential colleges reduced from 2000 to 7. Finally, using the information on college majors, only 1 college remained.

Part b.

The "anonymized" data released to public could reveal sensitive information about the people in the datasets- "Health insurance records" (Sweeney, 2002) and "Demographic, administrative, and social data about students" (Zimmer, 2010). Consider the example of "Health insurance records" dataset with patients' information like sex, ethnicity, visit date, diagnosis, etc. It was merged with the dataset on voting records in Cambridge city to extract the medical records of city's Governor William Weld. Sweeney combined the two different datasets using data fields like "Zip code", "Birth date" and "Sex", which were common to both the datasets. Then using birth date, zip code and gender of the governor, he successfully obtained the governor's medical records. Similarly, anyone can extract personal details of public figures whose zip code and birth date are public information.

In the case of "Demographic, administrative, and social data about students" dataset, the college was identified using information present in the freely available codebook and a search through an online database. After college identification, finding personal level details for students becomes easy using their friend network and cultural fingerprint, which are often unique to many individuals. Re-identification of certain individuals with a unique set of characteristics like ethnicity, race and hometown state is particularly easy. After re-identification of an individual, her/his sensitive information like cultural information, political views, etc. could be extracted from the given dataset.

Question 2. Describing ethical thinking

After re-identification of the college of "Tastes, Ties and Time" research dataset, Jason Kaufman, the principal investigator of the T3 research project[1], didn't offer an apology. Instead, he said that his research team comprised of Sociologists and technology (in terms of data re-identification, etc.) was new to them. His remark ''Sociologists generally want to know as much as possible about research subjects'' reflected consequentialism ethical framework wherein the focus is on the end result and not on the means to get the results. Kaufman didn't stop at this and instead argued that even if hackers cracked the research data that was made public then also there won't be any harm to the participants. He also explained that they neither did they collect any information about the participants which was not already available on Facebook, nor carry out any interviews or ask participants for any other information. It appears that he was trying to defend his consequentialist ethical framework by implying that the participants' Facebook profiles were as vulnerable to attacks from hackers now as they were before the study was conducted. He defended his team till the last moment by remarking "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)"[2]. The principles of "Respect for Persons" and "Justice" weren't followed while conducting the "Tastes, Ties and Time" research. An extra level of security in terms of data-privacy would have not only provided respect and justice to the participants but would have also helped the research work a great deal.

[1] Zimmer, Michael. ""But the data is already public": on the ethics of research in Facebook." *Ethics and information technology* 12, no. 4 (2010): 313-325.

Question 3. Ethics of Encore

Part a.

Narayanan and Zevenbergen (2015) made an assessment of Burnett and Feamster (2015) Encore study from "the ethical, benefit-harm, consent, transparency, and legal perspective"[2]. The researchers of Encore study ran a code from the web browser of any user who happens to visit particular web pages. The code would then perform censorship measurement by accessing content of a given list of potentially filtered websites. The underlying sequence of website visits and information retrieval (in form of identifying if the websites are blocked or display modified contents, etc.) would be invisible to the user of the system and Encore would automatically send the collected data to research team's server. Encore study subscribes to ethical framework of consequentialism as Narayanan and Zevenbergen (2015) assessment highlights that the study "generates significant positive benefits with some potential harms that can be mitigated"[3]. Given the balance between benefits and risk, the researchers undertook actions to study censorship worldwide, thereby focussing on the end result. If they were to follow the deontologist framework then they wouldn't even have conducted the study altogether as the study in its current framework doesn't respect the autonomy of the participants.

Also, the Encore study did fairly well in following the principle of Beneficence. The principle of Beneficence requires the study to not cause any harm to participants but if in case, some risk is involved then the researchers should maximize possible benefits while minimizing possible harms. The study exposed its participants to unwarranted risks as noted in Narayanan and Zevenbergen (2015) assessment, "users downloading censored URLs might face repercussions if they live in a regime without due process"[4]. Overtime the researchers engaged themselves in discussions with other experts/researchers to improve their study. In order to mitigate some of the potential harms, they collected data only from social media sites like Facebook, Twitter, etc. A risk/benefit analysis of such a large scale study which is being conducted in a complex environment of the Internet along with rules and regulations of different nations is very difficult. The Encore project didn't follow the Principle of Respect for Persons as it didn't seek any consent from the user whose Internet Protocol (IP) address was used to access content from different websites. One could argue that there's' wasn't a human-subjects research under the standard definition used by IRBs so a consent wasn't a necessity, however, the Menlo Report interprets human-subjects research as "human-harming research" also. And initially, the study did expose the participants to potential harm. Narayanan and Zevenbergen (2015) assessment didn't find Encore study to be unethical or in violation of any US laws but noted that the study could have been made more transparent by seeking consent from the participants.

[2, 3, 4] Narayanan, Arvind, and Bendert Zevenbergen. "No encore for Encore? Ethical questions for web-based censorship measurement." (2015).

Part b.

Burnett and Feamster (2015) Encore studied internet censorship by targeting IP addresses of users who happens to visit a particular website. Their code then sends information retrieval requests to a bunch of websites and then sends a report to the research team's server. Encore study didn't follow the principle of Respect for Persons as it didn't ask for consent from the participants who unintentionally happened to participate in the study. They used their IP addresses to connect to different websites without their knowledge and permission. Encore study did fairly well in terms of respecting the Principle of Beneficence as they continuously modified their research study in order to mitigate risk to the participants by discussing their study design with other experts. As requesting some of the Uniform Resource Locator (URL) could be incriminating at some places, the research team eventually restricted data collection only from social media sites like Facebook, Twitter, etc.

A risk/benefit analysis involving multiple laws and legislative regulations of multiple countries; and the complex structure of the Internet wasn't feasible. The researchers could have modified the user IP address while setting up connection with websites so as to avoid any harm or unwarranted repercussions to the user. As the study didn't target participants based on any vulnerability, it followed the principle of Justice. Under the principle of Respect for Law and Public Interest the study met the requirement of transparency based accountability as it itself asked for reviews from two different IRBs and engaged in discussions about research ethics by publishing their research study and not their results. Encore study lacked compliance as it didn't take steps to find out if it was violating any international laws or laws of a given country. Briefing the participants about the research and its methods in addition to seeking their consents would have made the study ethically conformable. In the starting period of research, the researchers followed the ethical framework of consequentialism by focussing on the ends. However, researchers' engagement in discussions on ethics in similar research studies and consultation with ethics experts to mitigate risk to the participants tries to strike a balance between the two ethical frameworks: consequentialism and deontology.

References

Sweeney, Latanya. "k-anonymity: A model for protecting privacy." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, no. 05 (2002): 557-570.

Zimmer, Michael. "“But the data is already public”: on the ethics of research in Facebook." *Ethics and information technology* 12, no. 4 (2010): 313-325.

Narayanan, Arvind, and Bendert Zevenbergen. "No encore for Encore? Ethical questions for web-based censorship measurement." (2015).

Burnett, Sam, and Nick Feamster. "Encore: Lightweight measurement of web censorship with cross-origin requests." In *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, pp. 653-667. ACM, 2015.