Assignment 8

Q1: Identification risk in anonymized data

(a) The examples I pick are: "Credit Card Transaction Data" from Montjoye et al (2015) and "Demographic, administrative, and social data about students" from Zimmer (2010). Both datasets are subject to substantial risk of re-identification attack due to similar structures. Although researchers mightly have made efforts to mask the data and protect the participants' privacy, the "unicity" of these datasets expose themselves to substantial risks (Montjoye et al, 2015, p537). The T3 data, for example, revealed its unique subject majors, which is consistent with what Harvard College offers; and once the population is narrowed down, it would take little effort to identify individual students by tracking their unique social network footprint. The credit transaction data, with outside information, it is easy to deanonymize the dataset since each client has their unique transaction records. Both datasets suffer from too much of spatiotemporal information, which lends them enough uniqueness to be de-anonymized.

(b) In the case of "Credit Card Transaction Data", the clients' historical transaction data may be leaked. Adverse parties can easily identify any individual in that dataset if they know some spatiotemporal information of that individual. Mobile transaction data contain rich information about one's financial status, work, consumption, which could be utilized for unfriendly purposes. Besides, according to what Montjoye said, "a survey shows that financial and credit card data sets are considered the most sensitive personal data worldwide." (Montjoye et al, 2015, p537) Disclosing these data will most breach their privacy in a subjective manner.

For "Tastes, Ties and Time", the identity of both the school and its students are exposed to information leakage. Since the school has unique subject majors and special housing policies ("one has to pick 1 to 7 best friends to live with throughout their college life"), Harvard College is quickly revealed among thousands of possibilities. Conditional on this, every student active on Facebook networks are easy to identify. And the data speak about their "friendships and cultural tastes, academic majors and where the students lived on campus." (Zimmer, 2010)

Reference

Montjoye, Yves-Alexandre de, Laura Radaelli, Vivek Kumar Singh, and Alex Sandy Pentland, Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata," *Science*, 2015, 347 (6221), 536-539.

Zimmer, Michael, But the Data is Already Public: On the Ethics of Research in Facebook," *Ethics and Information Technology*, 2010, 12 (4), 313-325.

Q2: Describing ethical thinking

Kaufman's argument centers around the beneficence principle, which essentially requires researchers to adequately balance between risk and benefits of a research. (Salganik, Matthew J., 2018) Kaufman and his team believe they have generated an unprecedented dataset that is objective and always on, that will magnificently empower sociologists to do their study, especially those who are interested in social networks. The ability of their dataset to answer social science questions should balance well against the risk of re-identification. Although they act in consistency with IRB rules, this principle asks for more effort in improving risk/benefit profile of this project, instead of just reaching an arbitrary balance. Besides, this argument breaches the “Principle of Justice”. Risk and benefits are not fairly distributed, as Harvard College students bear all the harm of being identified and it is the sociologists who benefit most from such data release. In general, Kaufman follows a consequentialism framework, where he argues that the anticipated fine outcomes as a whole will justify researches on this data.

Kaufman also defenses their project by saying that hackers who have adverse intent to make use of students' personal information will directly go for Facebook, and they did not add any personal information beyond Facebook.

From a consequentialist perspective, they are not worsening the potential minimal risks and at the same time fostering new research. But deontology thinking will refute the argument. One deontology principle that gauges ethicality is "Respect for Persons", which requires, if possible, informed consent from the participants. In addition, researchers should discern between their use of Facebook data and relevant laws, terms-of-service. Prudent decision should be made upon whether their acts violate any of the regulations or contracts, otherwise they will be defying the principle of "Respect for Law and Public Interest" (Salganik, Matthew J., 2018) The researchers should have felt uncomfortable if they put themselves into the shoes of a Harvard College student and they should, therefore, be more cautious about privacy protection strategies.

Reference

Zimmer, Michael, But the Data is Already Public: On the Ethics of Research in Facebook," *Ethics and Information Technology*, 2010, 12 (4), 313-325.

Q3: Ethics of Encore

(a) Encore is a system deployed across the global internet that can make cross-origin requests to measure "web filtering without requiring users to install custom software, enabling longitudinal measurements from many vantage points." (Burnett and Feamster, 2015, p653) However, the implementation of the system is not subject to participant "affirmative consent" and therefore strikes a dispute over ethical norms of "computer networking and Internet measurement research". (Narayanan and Zevenbergen, 2015, p2)

The construct of the Internet has enabled researchers to track and measure user and network behavior without explicit notice. Part of this possibility is due to some unintended security holes which might be taken advantage of. This would make the research, or any other forms of exploitation unethically intrusive to user privacy and relevant rules. On the other extreme, opponents espouse zero interference to personal devices. (Narayanan and Zevenbergen, 2015, p4)However, Encore project falls on neither of the realms. While refraining itself to appropriate uses of techniques, the project challenges the tradition of 'human subject study' to maintain a limited size of experiments. Encore is incredible for its scalability and 'stealth', which can present rich resource to study censorship mechanisms.

According to what is advocated by Salganik (2018), the principle of beneficence requires discreet analysis of the risk/benefit profile. To proceed with a thorough analysis of the project's ethical quality, the framework proposed by Menlo Report is followed, which makes an resemblance to what Salganik (2018) define as Consequentialism thinking:

First, guidelines of Menlo Report call for a 'systematic and comprehensive' analysis on who the stakeholders of the project are. Literally, every Internet user might involve the study and benefit or lose from it. The scalability of this project jeopardizes the possibility to implement such analysis on individual stakeholder. Besides, it is undetermined whether the project could be categorized as a human subject research since web users are not directly the 'objects' being studied. But admittedly participants are likely to be negatively affected, with their configured browsers sending secret requests.

Second, they tried to depict the risk/benefit profile of the entire project. It is not viable to implement the risk/benefit analysis on the individual level since their contexts vary across nation, religion and other 'social factors'. In contrast, the world of research can gain substantially from the project. It aids to revealing 'motivation and technology behind censorship', which in the meantime mitigate technical concerns and shed light on how to bypass such censorship. In respect to risk, 'minimal risk' analysis is performed, which makes a typical example of consequentialism thinking. It essentially contrasts risks associated with the project against risks without or what routines impose on people. Narayanan and Zevenbergen (2015) imply that the project might be more consequential than what its initiators presumed. Sending requests to third-party websites is likely to be at odds with users' intents, and might trigger severe surveillance personally, or to an even broader scale. Researchers may have also underestimated the severity of visiting prohibited domains under certain regimes. This risk/benefit profile clash with the 'Justice Principle'

(Salganik, 2018), since benefits and risks are not shared fairly.

Third, to assuage harms made to participants, it is vital to conform to norms regarding "informed consents, transparency and accountability". Much of the ethical dilemma could be resolved with informed consents from users, although researchers contend that it is impractical and undesired. Encore has taken sufficient measures to make their project specifications accessibly transparent, and clearly complies with US laws. But more legal advice is needed to tell if they have entailed infringement on local laws overseas.

To wrap up, from a consequentialist standpoint, it is unclear Encore harmonizes with ethical conventions, since outcomes are hard to anticipate or even define. The project serves a typical case where "technical experiment design" and beneficence analysis get so complexly intertwined. (Narayanan and Zevenbergen, 2015, p16)

(b) Here I will try to combine both consequentialism thinking and deontology, together with the four principles proposed in Salganik's book (2018). In general, I consider the ethical quality of the Encore Project very problematic. Consequentialism "focuses on taking actions that lead to better states in the world" (Salganik, 2018), which is achieved either through a reasonable equilibrium between risks and benefits. This resonates what the Principle of Beneficence demands. Despite the breakthrough quality in its technical design, Encore fails to appraise the danger faced by participants and minimize the risks they bear. Besides, Encore's "Respect for Law and Public Interest" is constrained within US most mundane networks such as Facebook and Youtube, but is likely unsolidified once the project is extended. Furthermore, in view of its deontology quality, Encore indicates deficient "Respect for Persons" and ignores participants' personal intents and safety under extreme regimes. Censorship measurements might endanger some people to harsh surveillance and inspection, or even paralyze the entire network connectivity. The system, undeniably, is gearing towards more risks imposed on Internet users.