Dhruval Bhatt
MACS 30000, Dr. Evans
December 3, 2018

Part 1: Identification risk in anonymized data

Re-identification attack, where an individual can be identified from an anonymous dataset, is a serious threat to using and distributing large sets of data that are collected by researchers using new technology. Two examples selected from the given set of examples, "Credit card transaction data" and "Demographic, administrative, and social data about students" illustrate how re-identifying individuals can be relatively simple. In both cases, data was anonymized based on existing minimal standards, that is, the name, emails, account numbers and other obvious identifications are removed. Financial data in "Credit card transaction data" by Montjoye et al. can be reidentified by spatiotemporal points such as where was the transaction made and when. In addition, the price of the transaction can aid in reidentification. Whereas in the "Demographic, administrative, and social data about students" example by Zimmer, a part of the reidentification was carried out by correctly deducing the anonymous, just based on the codebook and public comments. Knowing that the type of institution, narrowed location (New England region) and how many students were in the initial class (2009), it was possible to narrow it to a few colleges and with the information on majors, the actual college was pinpointed. Additional student information about gender, interests etc would have made individual identification easy. In both cases, information about location and time is important in reidentification. Additional details further aid in re-identification.

In both cases, the data is initially anonymized to protect people's privacy. However, with this relatively easy re-identification, sensitive information about people could be revealed. In case of credit card data, once an individual is identified it is easy to know where the person might be at what time. That is, one can be found at a particular coffeeshop at a certain time. Or what has that particular person bought recently revealing their needs and basic purchasing habits which could be used to infer future needs and habits. For the university data, knowing the individual's information, a person's "culture fingerprint" is revealed. Information about one's social preferences and tastes will be freely available, and it could lead to distress without any consent if it is made public. Additionally, tying that to university data of students' residency is telling about life lived offline.

Part 2: Describing ethical thinking

"We're sociologists, not technologists, so a lot of this is new to us and `Sociologists generally want to know as much as possible about research subjects."'

> **Rewrite:**
> "As Sociologists we want to know as much as a possible about research subjects to ensure that the research we produce provides widespread benefit to all, including the students themselves, and causes the least harm possible."
>
> **Explanation:** The statement made by Kauffman does not justifiably answer the principle of Beneficence, that is the benefit associated with a study should outweigh the risk and

Justice, that a small group of people are not unfairly burdened by the risk to provide benefit to another demographic. The rewrite shows that the researcher is aware of this vein of thought.

“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.)"

Rewrite:

“While hackers could gain access to any of the information from this study on their own through Facebook and may have little use to such information, the research subjects are the ultimate owners of their own information and preferences and their consent is important.”

Explanation:

Kauffman takes an approach that the research subjects are not harmed or at least not subject to more harm than they already could have been but does not factor in the ethical principle of respect for persons, that is, humans are autonomous beings and their explicit consent is necessary for using them or their information. If there is a major gain from getting the data without consent, that should be explained and not treated lightly.

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)."

Rewrite:

“We have not intentionally accessed information that is not publicly available nor exposed information gained by interviewing or asking about the participants. However, we have taken added precautions to anonymize data as some information was available only in network and can take additional measures to ensure consent”

Explanation:

While the researchers have used publicly available information, the do not acknowledge the fact that the information was available for different reasons. People posted the social information to share with friends not participating in research. This once again brings up question of the principle of justice, is it fair that a small group of people lose their protection of freely socially express themselves? Especially since the researchers used in-network research assistants, the researchers decided for the participants that all information posted will now be available to all.

Part 3: Ethics of Encore

To explore the question of ethics in computer science research, in particular, research on web-based censorship, Narayanan and Zevenbergen analyze the research project Encore by Burnett and Feamster. This project is a measurement tool for internet censorship and operates by utilizing code added to a user's web browser upon visiting certain cites and tries to request access to restricted sites to measure censorship. This is done without the consent or explicit knowledge to individuals. In this critique by Narayanan and Zevenbergen, they explore the ethical constraints on this project and hope to illuminate the principals over ethical dilemmas are determined. One aspect the authors point out is the use of program committee in determination of the ethical concerns of computer science research as opposed to dedicated review boards in medical and social science. The hybrid nature of human and technology in internet, puts it in a gray area when impact on humans is considered.

In a following discussion, Narayanan and Zevenbergen analyze the Encore project in the structure of Menlo report, a guide to ethics principles in computer science. The authors recognize that the stakeholders are wide and varied. Anyone using the internet could become a participant. This is what the computer science researchers want – to be able to scale to large population with minimal interference or control. However, this is not typical of other human-subject based research where one wants to minimize the human participation. This inherent difference in approaches creates a conflict in ethics guidelines for a technology-based project that impacts humans. Additionally, the authors explore the issue whether Encore study can be categorized as human subject research or not. They present Princeton and Georgia Tech IRB's argument that is not human subject research as it does not involve direct collaboration with humans. While notes from Office of Human Research Protections suggest that IP address can be considered as PII for an individual by HIPAA and other EU directives. This means that, though Encore is primarily researching the censorship network, using humans to generate the data, makes the research accountable to ethics standards.

Narayanan and Zevenbergen go on to discuss the risk/benefit analysis of the study and how to mitigate any potential harm. The study is clearly beneficial in understanding technical mechanism of censorship and demystifying it to reveal any potential human rights violation. Though they also recognize that the censorship standards are different and in case of a global project, global laws and beliefs must be considered. While there are benefits the risk is high too. People in some countries may suffer severe penalty for access to certain websites. A pure consequentialist approach cannot be taken as even if the result is beneficial, some people could be seriously harmed. While discussing the beneficence, it is important to mitigate the risk to justify the study. While the researchers of Encore believe that informed consent would put people at great risk with certain governments and reduce the ease of scalability of the projects, many committee members believe that might actually address some of the risk concerns. Even though the Encore project is in legal compliance in the united states, further investigation and understanding of global laws is important. Such analysis and ethical considerations will become more important as global, internet-based projects become more prevalent in society.

Ethical quality of Encore study

The ethics of Encore study have been widely talked about as it has revealed challenges of large scale, global studies that can be conducted through internet with little to no involvement of computer users. The research was declined from IRB reviews as it did not collect and analyze Personally Identifiable Information (IIB) but even then, the researchers did not shrug away all responsibility to explore the impact of their work through the ethical framework. The authors of the Encore study explicitly discuss ethics in their publication. They review their thought process on the benefits of this tool in censorship measurement and associated risk. They also discuss the question of informed consent and explain why it is not best not sought in this situation. The authors have made good efforts to think about and minimize the risk transferred to the unsuspecting users of Encore. In that regards, this is study has high ethical standards. The arguments are not made simply to cover themselves from any legal implications but debated to uphold the principles of ethics. However, the concerning effects of the study are not completely unjustified. This tool could put individuals at risk with repressive governments and it is an intrusive tool in other governments' operation. On that basis, it is best to further gain clarity as to how to handle that risk before large scale deployment. Due to the benefits offered, I believe it is not unethical to use the tool but to reduce the risk, approval and ideas from legal institutions from different countries would be advisable.