Assignment 8

1. Identification risk in anonymized data

(a)

I pick Health insurance records from Sweeney (2002) and Netflix movie rating data from Narayanan and Shmatikov (2008). In these two cases, the re-identification attacks share a similar structure. Specifically, there are two datasets, one containing sensitive information of individuals but no personally identifying information, the other containing personally identifying information but no sensitive information. The two datasets share some common fields, by which one can merge these two datasets and combine personally identifying information with sensitive information. In this way, one can pin down sensitive information of a specific individual.

(b)

In Sweeney (2002), there is a medical dataset containing individuals' medical information like the medical visit date, diagnosis, precedure, medication, and total medical charge, which are potentially sensitive. This dataset doesn't include identifying information, but contains individuals' ZIP code, sex, and date of birth. The author also had access to "the voter registration"(Sweeney, 2002:p.2) data, which includes people's names together with ZIP code, sex, and date of birth. By merging these two datasets by the common fields (ZIP code, sex, and date of birth), the author was able to get the medical information of a specific person (William Weld, governor of Massachusetts).

In Narayanan and Shmatikov (2008), the Netflix movie rating dataset contains people's rating to movies, and personally identifying information like name has been removed. But if an adversary has some information(not required to be perfectly accurate) about when some individual rated a specific movie and the corresponding rating, there's a large possibility that the adversary can identify this individual's record in the Netflix movie rating dataset, and get access to this individual's sensitive information, for example, political preference.

2. Describing ethical thinking

According to the principle of beneficence, researchers should balance the benefits from the research and potential harms to research subjects (Salganik, 2018: p.296). As sociologists, Kauffman and his coleagues wanted the dataset to include more details so that they could create more new knowledge by studying the dataset. However, more personal information in a research dataset is dangerous to the subjects of the research because there's a higher probability that their personal information gets identified and their privacy gets hurt. So Kauffman and his coleagues should have better balanced the gain from the data and the potential harm to the students.

By commenting that hackers could also get people's private information directly from Facebook, Kauffman was arguing from a consequentialism view of ethics. Although the procedure of building this Facebook dataset might be ethically questionable, but the consequence was just that the students' information that was already available on Facebook, was included in the dataset. From a consequentialism view, this doesn't make any difference since those who want to crack the data can get the same information from Facebook.

By stressing that they only included the information on Facebook and that they had never interviewed anyone, nor disclosed any subject's privacy, Kauffman was arguing from a deontology view of ethics. During their research, they showed respect to people's autonomy and privacy, so they didn't do any interview and only included public available information. They tried their best to protect the content of the dataset. But if someone successfully cracked the dataset and made use of it to do harm to the subjects, it should be the hacker to blame, not the researchers, since they had done their ethical duties.

3. Ethics of Encore

(a)

The controversial censorship measuring project Encore is discussed in Burnett and Feamster(2015). Encore injects "an invisible element into the page, which will then instruct the visitor’s browser to download and execute a piece of code"(Burnett and Feamster, 2015: p.2). This code will let the browser send requests to some websites without informing the user, see whether they are successful, and send the results to the researchers. Despite being a efficient, scalable strategy and having collected valuable large-scale censorship data around the world, Encore still faces an ethical dilemma.

Some intrinsic features of the internet have allowed computer science researches to keep track of internet users' behaviors "without affirmative user consent"(Burnett and Feamster, 2015: p.4). Some of them are highly contraversial because they make use of internet security holes, while Encore, probes devices on the internet without "exploitation of any security holes" (Burnett and Feamster, 2015: p.4). Other features like avoiding hiring volunteer or government intervention, and producing global-wide fine-grained data in a scalable and automatic way, make Encore even more technically attractive. However, as the committee of "ACM SIGCOMM 2015"(Burnett and Feamster, 2015: p.7) pointed out, there are three ethical problems in Encore. First, being a "third-party requests used for ad tracking"(Burnett and Feamster, 2015: p.7), Encore should have informed the users. Second, it potentially exposes the users in the risk of being punished by the regime if their online activities are monitored; Third, if the users were actually informed, they "would be unlikely to consent"(Burnett and Feamster, 2015: p.7) since they live under censorship.

To analyse the ethical issue of Encore, the authors follow the framework of "the Menlo Peport" (Burnett and Feamster, 2015: p.8).

First, to answer "who are the stakeholders"(Burnett and Feamster, 2015: p.9) of Encore is difficult because when the "user’s browser sends a request to a potentially censored website", "the user’s IP address may be recorded by the server hosting that website", "many intermediaries and potentially unknown third parties", and also "the Encore research team" (Burnett and Feamster, 2015: p.9), and potentially the regime that performs censorship.

Besides, trying to identify the stakeholders is in confliction with the scalability goal of Encore because it involves millions of devices "used by humans who are not themselves the direct subjects of research"(Burnett and Feamster, 2015: p.10).

Second, to answer whether Encore is a "human-subjects research"(Burnett and Feamster, 2015: p.10) is also hard. "Neither the Princeton nor the Georgia Tech IRB considered Encore to be human-subjects research"(Burnett and Feamster, 2015: p.10) because it neither involves "intervention or interaction with individual", nor includes "identifiable private information" (Burnett and Feamster, 2015: p.10). However, whether IP address should be considered "identifiable private information" is under debate.

The benefit of Encore is more clear since it provide data for censorship measurement such that researchers can study the motivation and technologies of censorship. However, despite the general negative attitude towards censorship among researchers, many also question the use of "big-data" in censorship measurement arguing that most of these measurements are biased and causal inference is sometimes arbitrary.

On the other hand, it's difficult to assess, or even define, the potential harm of Encore to individual internet users "due to the complex, dynamic, and innovative nature of the Internet" (Burnett and Feamster, 2015: p.11). From a consequentialism view, the authors of Encore argued that the risk of Encore should be compared with the "minimal risk" which people face in their daily life. And they claimed that even without Encore, people are exposed to the risk of third-party tracks. However, others argue that researchers "should not participate in and facilitate a race to the bottom"(Burnett and Feamster, 2015: p.13). Also, the harm to users can vary with "the type of censored websites"(Burnett and Feamster, 2015: p.13) Encore direct the users' browser to. Besides, the censors' responds are out of the researchers' control and can lead to unexpected harms to the subjects.

Burnett and Feamster(2015) also analyse how the harms of Encore can be mitigated in terms of "informed consent, transparency and accountability"(Burnett and Feamster, 2015: p.14). The major ethical defect of Encore is the absense of informed consent. However, obtaining it can be technically difficult, reduce the architectural benefit of Encore, and put higher risks on the users. As for transparency, Encore provides website operators with a instruction on how to inform visitors of Encore and provide the option of disabling it, but they are not required to do so. The legal compliance of Encore is complicated because it involves machines around the world so the researchers can't be completely sure that they are not violating any law of any region.

(b)

I will assess the ethical quality of the Encore project according to the four principles in Salganik(2018). First, Encore does not show enough respect to persons. Although the researchers provide a description of the project on their website and allow users to opt out of it, Encore doesn't ask for the consent of the users everytime it direct the browsers to potentially censored websites. Most users are not even aware of it, which violates the principle that people should be treated as autonomous and their wishes should be honored. Second, balancing the benefits of the research and the harms to the subjects is intrinsically difficult in this project. Censorship measurement might bring harm to people involved if they live under a regime that strictly regulates people's online activities. However, how can we fight against censorship if we

don't understand them politically and technically? Third, in terms of justice, the risks and benefits of the study are not distributed fairly since Encore involves people living in different censorship systems. However, it is beyond the researchers' control if they wish to keep the global feature of the study. Finally, Encore shows some respect for law and public interest by making the project transparent. But it's hard to conduct a systematic legal assessment of the project since it involves people in different legal systems.