Cosette L. Hampton

Assignment #8, MACS 30000

Fall 2018, Dr. Evans

Due: Monday, Dec. 3 at 11:30am

1. **Identification of risk in anonymized data (4 points).** 
   1. Two examples chosen: Search log data (Barbaro and Zeller, 2006) and (Zimmer, 2010).

In both cases, supposedly anonymized data was released that researchers were still able to use to identify people and groups. With the search log data, bloggers “…identified other AOL users by examining data,” or, “set[ting] up websites that let people search the database of searches” (Barbaro and Zeller, 2006). With the T3 project, researchers were able to identify the school of interest using the public profile Facebook data and similarly, “Individual bits of data that might have been added and modified on a subject’s Facebook profile page over time were harvested and aggregated into a single database…” (Zimmer, 2010). Individuals also did not provide informed consent and information was publicly accessible though “harvested for research purposes,” (Zimmer, 2010).

* 1. Sensitive information about people’s interests and conditions could be revealed using their search log data, and the possibility of identifying a user increases the more data is collected. They say that, “…the searches appear to betray (portray?) intimate emotions and personal dilemmas… [and other queries] that raise questions about what legal authorities can do with such information.” (Barbaro and Zeller, 2006). In the T3 project, data acquired were: “…the subjects’ self-reported gender and ethnicity, but also their home state, nation of origin, political views, sexual interests, college major, relational data, and cultural interests—data which would be considerably more difficult to obtain through observations in a public square.” (Zimmer, 2010). The cultural data released by T3 in particular could expose information about students that could impact public image (i.e. fellowship/job/school applications) if accessed, and the same can be said for search log data, which could also spread embarrassing information about people or make them subject to harassment. Three key areas of violation discussed by Salganik that are relevant here are informed consent, privacy and “understanding and managing informational risk,” (Salganik, 2018).

1. **Describing ethical thinking (3 points).**

After the school of interest was discovered to be Harvard University, attracting criticism of research team’s lack of ability to protect the privacy of the people researched in the study, Jason Kaufman, the principal investigator of the T3 research project reacted quickly and responded to critics, explaining that the researchers are sociologists who want to know as much as possible about research subjects and do not have a lot of technical background to be able to understand that by using some technical processes, other researchers may be able to identify their subjects, thus putting their privacy and autonomy at risk. Essentially the T3 team did the best they could in order to protect the privacy of the human subjects and follow guidelines about collecting data while still doing robust research, especially since they did go through an IRB approval process. These points are in-line with Salganik’s principles of “Respect for Law and Public Interest” since they attempted to obey terms of use and “Beneficence” because they thought benefits would be maximized by having as much information as possible (i.e. housing data and Facebook profile data) (Salganik, 2018).

Kauffman continued to attempt to diffuse privacy concerts, stating that there would be no difference in risk of exposure to hackers because the same data they used for the T3 study could also be collected via Facebook itself because privacy filters are easy to get around. Further, they did not actually contact anyone or made information about people public, which they took special precaution to make sure that most people would not be able to gain information about people simplistically. The first point here relates to Salganik’s discussion of consequentialism and “Respect for Persons,” where because the Facebook information was already public there was no risk in using it on the end of the subjects—to T3, by putting the information on Facebook people consented to having their information out there. Additionally, like earlier, they attempted to follow terms of service by not getting information that is beyond the reach of the public Facebook profile as discussed according to compliance (Salganik, 2018).

The second point relates to, perhaps, a violation of compliance and “transparency-based accountability” (Salganik, 2018) of the individual(s) that de-anonymized the data, since they did, “…[require] other researchers to agree to a ‘terms and conditions for use,’ prohibiting various uses of the data that might compromise student privacy…” (Zimmer, 2010). Basically, the people who used T3 data violated T3’s compliance agreements when they took special interest to find out who the students were, and they violated transparency-based accountability when they announced that the school of interest was Harvard University.

1. **Ethics of Encore (3 points).** 
   1. **See below:**

User-analytics uses various tools to gain data on various topics without having subjects’ informed consent. Some are intrusive, like “Spamalytics” or “Carna” that actually went into people’s machines, while others that use data of providers like the Internet Service Providers (ISPs) are more observational in nature. The Encore study used both methods by exploiting the structure of the web and ad impressions to measure censorship.

Narayan and Zevenbergen consider this, and “ethical and legal questions” when making their assessment of the Encore study. To them, researchers themselves should be guided by ethical principles that are not invasive without consent, but IRB processes also need to consider their own evaluation as having loopholes, because reviews are done after the research has already taken place so unethical activity isn’t prohibited at the outset of the research project, but it can also prime researchers to avoid or abandon some research questions that do not actually have unethical methods for worry of IRB rejection. Finally, some projects may not even be evaluated by IRBs because they are not considered “human subjects” research because researchers do not engage with people, even though people’s information is being used in the study.

With regard to Encore, Narayan and Zevenbergen consider consequentialism and the principle of beneficence that focus on research that is done to “…[take] actions that lead to batter states in the world… [and] balance risk and benefits…” (Salganik, 2018) of research processes. They state that because measuring censorship helps illuminate censorship, it “…yields valuable insights in political science… [and] enhances the ability to create effective censorship circumvention tools [44].” (Narayan and Zevenbergen, 2015) Basically censorship is seen as more harmful than tracking censorship because censorship itself is a human rights violation of freedom of speech and information. Technologically, censorship “…inevitably cause[s] network errors and security problems.” (Narayan and Zevenbergen, 2015) In the Encore study, the “bad” thing is the censorship itself and it is argued that the research is helping push back on the bad thing—perhaps there is no way around certain ethical violations when attempting to study issues that violate human rights themselves.

Finally, the risk in this does not outweigh the benefit, because, “The authors argue that normal web browsing exposes users to the same risks that Encore does…” ((Narayan and Zevenbergen, 2015). Some points of contention are raised relative to “users’ expectations” or informed consent again, or harm that may arise from repressive governments if it were found out that users were attempting to access censored/banned websites or blocked domains. According to Salganik, these people in these areas with repressive governments would be considered more vulnerable so reducing harm against them under beneficence also includes concepts of Justice so that they are protected even more within countries that censor. To Narayan and Zevenbergen, this protection looks again like, “Informed consent, transparency and accountability.”

* 1. **See below:**

Sometimes ethical considerations and requirements can prime certain behavior in the research subject population. In the case of the Encore study, informing participants that their visited websites would be monitored or attempting to attain consent from them may prime them to not visit censored sites at all for fear of being persecuted. Additionally, like T3, Burnett and Feamster (2015) did work with an Internal Review Board (IRB), so they were compliant and transparent in their research process. Perhaps though, they could have done better with regard to Justice by eliminating subjects that lived in countries that are very repressive as Salganik advised in Section 6.4.2, or not take observations in those countries at all. To follow Respect for Law and Public Interest, researchers, “…need to be clear about the goals, methods, and results at all stages of their research process and to take responsibility for their actions.” (Section 6.4.4; Salganik, 2018). The research of Encore was on “web filtering,” a technical process and not necessarily about the censored websites and their users, so going this deep with data of those who are vulnerable may not have been necessary to attain information about web browsers and filtering and test the hypotheses. For example, perhaps they could have set up their own randomized filtering system to synthetically test “webmasters” and “cross-origin requests” (Burnett and Feamster, 2015) instead of using real-world data.

**References**

**Barbaro, Michael and Tom Jr. Zeller**, “A Face Is Exposed for AOL Searcher No. 4417749," *New York Time*s, August 9, 2006.

**Burnett, Sam and Nick Feamster**, “Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests," 2015.

**Kauffman, Jason**, “I am the Principle Investigator...," Blog Comment, MichaelZimmer.org, http://www.michaelzimmer.org/2008/09/30/on-the-anonymity-of-the-facebook-dataset/, Sep. 30, 2008b.

—, “We did not consult...," Blog Comment, MichaelZimmer.org, http://www.michaelzimmer.org/2008/09/30/on-the-anonymity-of-the-facebook-dataset/, Sep. 30, 2008c.

**Narayanan, Arvind and Bendert Zevenbergen**, “No Encore for Encore? Ethical Questions for Web-based Censorship Measurement," *Technology Science*, December 15 2015.

**Salganik, Matthew J.**, *Bit by Bit: Social Research in the Digital Age*, Princeton University Press, 2018.

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