RDS Privacy Workshop

Case Study Materials

Cases for Analysis Exercise:

- Facebook Emotional Contagion Study (2012)*
- InBloom Student Privacy (2014)*
- 23andMe Genetic Privacy (2008)*
- Period Tracker Apps vis-à-vis *Roe* (2022)

** Adopted from Deirdre Mulligan, et. al., from CCC Privacy by Design Workshop, UC Berkeley, Feb 2015*

Facebook Emotional Contagion Study (from 2012)

For a week in 2012, researchers altered the algorithm that controls what comments from friends appear in a Facebook user's newsfeed to include consideration of its emotional content for a subset of users. Some users were exposed to increased positive content and others increased negative content. The content came from users' friends, and an algorithm was used to curate users' newsfeeds. The change involved how the algorithm determined what subset of information to place into the newsfeeds. Facebook's initial response stated that it complied with their privacy policy. However, they've subsequently revised their processes to address concerns raised by the research. Complaints about the study included:

> "the company purposefully messed with people's minds." (EPIC)
>
> "Facebook should not be manipulating people's data without their consent. What they did was really wrong."
>
> "You do not expect a company, providing you with a product or service, to try to manipulate your emotions and actions . . . to do something to someone unknowingly is still inherently wrong."
>
> "Most of the users of fb . . . have no idea they could become 'lab rats' using the information they shared privately. If they are going to do any type of psychological evaluation, it needs to be fully reviewed prior. . . . The terms of service] should read something like ' . . . we may conduct psychological studies based on your information shared."

Possible Questions to consider:

- What did the complainants want privacy to protect or safeguard? What was privacy's object here?
- Whose privacy does the complainant believe is being violated? Who is the subject of the information?
- What privacy related concerns might a user have if their messages were being selected to highlight their negative emotions for display in others' newsfeeds? What harms?
- What privacy related concerns might a user receiving a feed with more negative content raise? What harms?
- What action constituted or initiated the privacy harms?

Student Privacy at inBloom Inc.

The non-profit inBloom Inc. ran a data service that allowed school districts to manage student information with a goal to personalize learning and offer improved educational outcomes. inBloom grew out of a 2011 alliance to personalize classroom learning and received over $100 million in funding from the Gates Foundation, Carnegie Corporation, and others to take existing student data and aggregate it from multiple sources so that educators could gain central access and employ analytical techniques. The platform was able to store, clean, and aggregate student data, as well as make it available to third parties who wanted to develop tools and dashboards for classroom use.

The inBloom platform allowed education administrators to fill in over 400 data fields for student records, including data already collected such as grades, attendance, social security number, disabilities, etc. There were also options to include personal data about the family, for example, if the child had foster parents, or a parental figure was a "father's significant other." In addition, there were areas for subjective disciplinary terminology that described an incident from the perspective of the administrator using terms such as "bully" or "victim". There were also options for teachers to assign character traits to student profiles.

Protests and lawsuits in New York, Illinois, Louisiana, & Colorado caused many districts to back out of the contract.

In April 2014, inBloom announced the organization was closing amid waning confidence in student privacy practices and withdrawing state partners. Parents, educators, and legislators expressed concerns over the company's intention to share students' personal information with third party vendors. inBloom did not plan to ask for consent or give parental notification. inBloom's CEO expressed his disappointment to the press, and cited the organization's superior security standards that encrypted all data entered into the system by educators.

Experts have cited that many school districts in the United States use third-party vendors to manage student data, and these services often do not obtain parental consent and often lack appropriate security and privacy standards. The collapse of inBloom and rise of other firms with similar missions have led privacy advocates to call for improved student data protection regulations. For instance, student advocates call for greater penalties for violations of Family Education Rights and Privacy Act (FERPA) and for a Student Privacy Bill of Rights.

Comments about inBloom identified several concerns:

"Parents, not private companies, have the right to control personal information about their children. We should help student scholars make the grade, not help companies make a sale" - Senator Edward Markey

"There are more and more data-mining vendors who, with the help of government officials, foundations, and think tanks, are eager to make money off of student information in the name of "big data" and "personalized" learning and in the process see parents...as ignorant obstacles" - Parent activist L. Haison

"Ms. Barnes, the privacy lawyer, said she was particularly troubled by the disciplinary details that could be uploaded to inBloom because its system included subjective designations like "perpetrator," "victim" and "principal watch list." Students, she said, may grow out of some behaviors or not want them shared with third parties. She also warned educators to be wary of using subjective data points to stratify or channel children." – *The New York Times*

Possible Questions to consider:

- What did the complainants want privacy to protect or safeguard?
- What overall aims did they believe such protection served?
- Whose privacy do the complainants believe is being violated?
- What action constituted or initiated the privacy harms? What sort of harms are being claimed?
- What privacy concerns surround the use of predictive analytics on students? Would providing control over collection address them? How should educators and platform developers determine what data fields to include in student records?

Privacy and Genetic Material

As the cost of DNA sequencing continues to fall and the predictive power of genetics grows, the privacy implications become more pressing. In 2008 Congress passed the Genetic Information Non-Discrimination Act (GINA) which provides federal protections against genetic discrimination in health insurance and employment, but the law is not comprehensive in its legal protections for individuals who have received genetic testing. For instance if an individual has a genetic or family history of a neurological condition, this genetic data could be used against them during a lawsuit over a car accident.

23andMe began offering saliva-based direct to consumer genetic testing in 2006. These tests initially offered consumers an analysis of their genetic predispositions from over 254 diseases and conditions, and by 2014 they had data from over 800,000 individualis. The service was halted in 2013 by the Food and Drug Administration (FDA) over concerns regarding the public health consequences and implications from potential inaccurate results of the Personal Genome Services (PGS) and provided analytical results. Recently a biologist posted her 23andMe personal genetics story and how the PGS discovered her unknown half-brother, and caused a massive family rift resulting in her parent's divorce. This chain of events was precipitated by a default that opted users into a predictive relative finder program. The consequences (e.g., uncovering unknown or secret family) were not fully explained to participants. Further, 23andMe recently announced a deal to sell aggregated genetic data from their customers to the biotechnology company, Genentech. As part of the deal, 23andMe will be handing over 3,000 Parkinson's patients' and their families' DNA sequences along with extensive lifestyle and personality questionnaire answers.

Privacy protections centered on individuals exercising control over their own information have little impact on the implications of inferences applied to them but drawn from other peoples' data. Large complications of genomic data pose serious personal consequences for relatives – living, dead, or not-yet-born – as well as others who might share genetic makeup. The family of Henrietta Lacks, the woman whose cells were used without her consent to derive the HeLa cell line for medical research, recently came to an agreement with the National Institutes of Health (NIH). The NIH enacted a policy that gives the Lacks family some control over the full genomic sequence from HeLa cells after published medical research revealed the family had a predisposition to certain diseases.

Possible Questions to consider:

- Whose privacy interests were implicated by the biologists decision to have her DNA analyzed?
- What action constituted or initiated the privacy harms? What sort of harms are being claimed?
- What responsibilities do entities that collect genetic data that imputes connections have to those who are implicated by association?
- What current assumptions about protecting privacy might confound efforts to address the concerns above about genetic information?
- What options or defaults should be presented to consumers with regard to their genetic data in order to best respect their privacy and autonomy?
- What sort of technical approaches might prevent privacy harms flowing from genetic inferences?

Period-Tracking Apps and *Roe v. Wade*

There is a wide-range of period-tracking apps, with Flo (45 million active users) and Clue (12 million active monthly users) being among the most popular. Much of the data inputted by users are intimate (e.g., start and end of menstruation cycle, weight, sexual activity, etc.,), and information collected by the apps is not protected by HIPAA. This means the app makers are free to do what they want with the data they collect. Though these companies promised not to disclose details about "cycles, pregnancy, symptoms notes and other information that is entered by you" in January 2021, the Federal Trade Commission filed a complaint claiming they had sufficient reason to believe that Flo had misled users. The FTC alleges that between 2016 and 2019, the company behind Flo, provided information on the intimate health of its users to companies such as Facebook and Google.

The FTC's findings raise further concerns should the Supreme Court overturn *Roe v. Wade*. As of right now, privacy concerns primarily concern data being sold to third parties; however, with abortion posed to be banned—and potentially criminalized—in at least 26 states, this data, if subpoenaed, could be used to infer that someone has had an abortion.

Possible questions to consider:

- What privacy interests were implicated in the use of period-tracking apps?
- What options or defaults should be presented to app users with regard to the tracked data in order to best represent their privacy?
- What safeguards could the companies put in place so that the data is not at risk of being subpoenaed?
- What future ethical problems might this case raise in light of the changing legal landscape concerning reproductive rights?