Daniel B. Carpenter

CS 2334 - Project 5: Ethics

10 December 2020

Case 1: Privacy in a Global Pandemic

Three of many programming professional responsibilities include striving to achieve high quality in “processes and products of professional work,” accepting “professional review,” and performing work only in areas of competence.

According to “Apple and Google partner on COVID-19 contact tracing technology”, they plan to implement two mobile-phone technologies that aid in reducing the spread of the virus; these two technologies are application programming interfaces (API) and operating system-level technology. These two technologies allow for the tracing of the virus but could also provide risks to privacy. The second phase of Apple and Google’s plan includes the use of Bluetooth technology, which provides a more secure way to trace the virus. Within *A Gift of Fire***,** the author suggests the use of encryption like Bluetooth, which is a way of preventing the use of intercepted data, to combat privacy issues. It appears that Google and Apple did not implement Bluetooth in phase one due to time constraints, which ethically disbands privacy.

In support of using a less secure way to handle the pandemic, the code of ethics argues to “avoid harm,” which includes “physical or mental injury;” additionally, the code of ethics argues to “contribute to society and human well-being,” which includes “threats to health” and “safety” of the coder’s constituents. In the case of a pandemic, implementing a technology more quickly lessons physical injury, such as sickness or death, as well as benefits society by reducing health threats. However, the code of ethics also argues to respect privacy, which contradicts the above use of less-secure technology to slow the spread of the virus.

Regarding South Korea's approach to contact tracing, it appears that compromising between absolute privacy and foregoing freedoms could assist in South Korea's objective, while not materially affecting the outcome of their taken measures. Within the article "'More scary than coronavirus': South Korea's health alerts expose private lives," they discuss that South Korea implements a policy that reveals gender and age information in their tracing texts, which helps the individual understand where they may have received the virus. However, the government could avoid some of this ethical dilemma by not revealing the characteristics of individuals who were in contact with the texted individual. Although this alternative strategy could lessen the impact of their plan, it supports the code of ethics' sections' 1.4, 1.6, and 1.7, which respectively detail issues of discrimination, privacy, and confidentiality.

Case 2: 23andme

23andme's decision to sell the rights to a drug differs from Bluetooth contact tracing because it deliberately discloses consumer data for another's profit. The article discusses how 23andme developed a drug through consumers' voluntary decision to anonymously give their data for research, which appears to allow 23andme to sell the rights to their drug. However, selling this drug does not support ACM's code of ethics, section 1.7 in honoring confidentiality. This section clearly states research data "should not be disclosed," except in violation of the code or law.

23andme's ability to replicate a fingerprint from DNA data with precision provides both positive and negative externalities on society. Positive outcomes include the ability to help verify someone's identity, which could provide more secure authentication than something like a social security number. Additionally, replicating the methods they created could drastically improve the

research of other drugs or ideas. Alternatively, losing such data could increase identity fraud, which could devastate individuals' lives. Alongside that issue, selling that data could generate large profits, but again could hurt many people's lives.

The difference between the contact tracing and research data sale cases relies on ACM's sections that discuss avoiding harm, as well as honoring confidentiality. Although the contact tracing case only mentions Apple and Google's plan to contact trace, they do not explicitly say that they will use that data in malicious ways. In the 23andme case, 23andme does not act ethically by selling research data without the consent of the consumer. 23andme could have acted more ethically by following up with users and give them the option to sell the rights to their data while compensating them for 23andme's sale of data; 23andme likely did not implement this option because of loss of revenues from the sale, or potential expenses from distributing consent forms.

The company that obtains user data essentially owns the data, simply because they have a record of the information in their system. By only using necessary data, which excludes any sensitive information, in a team could help enable ethical practices. To ensure that an organization is acting ethically, the organization should implement policies like the ones discussed in *The Gift of Fire*. This book discusses implementing proper database security, as well as having recurring security audits from outside parties.

Case 3: Ethics in the Workplace

In the workplace situation, Alice and Bob to not "respect privacy" or being "honest and trustworthy," as discussed in the ACM Code of Ethics. The individuals do not respect the consumers' privacy if they are not communicating the uses of this personal data to the consumer.

Additionally, they are not honest or trustworthy if they are using the data for other reasons than intended. Alice and bob benefited Gaggle in this situation, which the company made a handsome profit from the inexpensive tracking service. All consumers using Gaggle could be harmed if Gaggle sells the data to a malicious company, such as a company that targets these consumers through unethical marketing practices. Making Alice's job easier may have motivated her actions. She could have assumed that being a whistleblower is not as easy as ignoring the issue and continuing to her next task.

Case 4: Open Discussion

Link to article: https://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html

Within the New York Times' article "How Volkswagen's 'Defeat Devices' Worked," the author discusses how the car company Volkswagen used computer programming to mislead regulators when conducting emissions tests. When emissions regulators tested VW's car, the car's software "sensed when the car was being tested," which then "activated equipment that reduced emissions." When the car drove without the emissions test, the car produced emissions far above "far above legal limits." Volkswagens' management implemented this software to either "save fuel" or improve acceleration.

This ethical dilemma violates sections 1.1, 1.2, and 1.3, which respectfully requires programming professionals to contribute to society, avoid causing harm, and to be honest and trustworthy. Volkswagen actively works against society by mass-producing cars that accelerate climate change. Volkswagen does not avoid harming others by implementing this software

because it produces harmful emissions that affect billions of people. Lastly, Volkswagen's programmers wrote this code only to be dishonest when conducting emissions tests, which violates section 1.3 of the ACM Code of Ethics.

First, I would ask the programming team who wrote the misleading emission software "did your managers coerce you to write this code?" Next, I would ask "if your manager coerced you to code the emissions code, did you try to stop this implementation?" Lastly, I would ask "if you could have seen this potential outcome, would you have still written this code?" These questions are important because it allows new programmers to understand that they could ruin their career by abiding by their manager's requests. Also, I think it would be important to understand how someone's decision would change if they understood the outcome.