Sean McLean

ITC 6000

Module 4 Homework

A recent story involving a data breach occurred with the ancestry platform 23andMe that led to a subsequent lawsuit last month. It was alleged by two plaintiffs that the company failed to protect the privacy of millions of users and then did not notify them of the breach until two months later. During that period, the information from the breach was shared and sold on other platforms. The data also targeted certain races including customers of Chinese and Jewish descent (Carballo, Schmall, Tumin, 2024).

The type of information that was stolen from the platform database was genetic data as well as user profiles and images. The hackers that caused the data breach used recycled login credentials like passwords that had been used on other websites (Carballo, Schmall, Tumin, 2024). The company offers DNA testing from saliva samples that its customers provide followed by an ancestral breakdown based off the test results. They provide several DNA testing packages as well as user memberships (23andme, 2024).

The data breach and following lawsuit has racial, social, and political implications as the hackers targeted particular users with the intention to harm and harass them. Many of the users including one of the plaintiffs in the lawsuit are of Chinese or Ashkenazi heritage and is being looked at as potential hate speech. The recent world events like the Israeli-Palestinian conflict have also increased safety concerns for certain racial minorities like Ashkenazi Jews. The lawsuit could also impact customer privacy laws due to the sensitivity of data breached and stolen from the platform (Carballo, Schmall, Tumin, 2024).

Some of the steps that the company should take from sources quoted in the article are to increase data security and limit the amount of data that the company keeps in its database (Carballo, Schmall, Tumin, 2024). Other improvements that the company could make in the future to avoid legal trouble are appointing a database security officer to ensure data integrity is a top priority for the platform. An area to look at is revising policies and procedures that focus on informing customers of a data breach immediately and what the protocol should be to prevent hackers from stealing any more data than what has already been taken from the website (Coronel, Morris, 2017).

This kind of story resonated with me from my past career in healthcare where we had several data breaches at the hospital that I worked at a few years ago. I worked in the health information management department where we were working with patient information every day. We were not the only facility that was targeted, and it was more of a data breach on a national scale, but working with sensitive and protected health information daily I was extra careful with patient protections and made sure to always be HIPAA compliant. We worked closely with our legal department when lawsuits were filed and had policies and procedures in place when issues arose that pertained to medical data breaches.

References

23andMe. (2024, Feb. 3rd). *How it works.* 23andMe.com. https://www.23andme.com/howitworks/

Carbello, R., Schmall, E., & Tumin, R. (2024, Jan. 26th). 23andMe Breach Targeted Jewish and Chinese Customers, Lawsuit Says. *The New York Times.* *https://www.nytimes.com/2024/01/26/business/23andme-hack-data.html?searchResultPosition=3*

Coronel, C. & Morris, S. (2017). Chapter 16. *Database Systems: Design, Implementation, & Management (12th Edition)*. Course Technology; 12th edition.