**CYB 260 Project One**

Douglas Few

Southern New Hampshire University

June 11, 2021

Privacy Laws

I don’t believe that current privacy laws are sufficient to ensure that the sharing of data meets the fair information practice principles of the organization. While privacy laws are put in place to ensure that information collection is done ethically, breaches and attacks still happen frequently enough to show that the law is not enough (Swinhoe, 2021). For example, in September of 2019, mobile game giant Zynga experienced an attack that impacted approximately 218 million user accounts (Zynga, 2019). Another incident occured in October of 2016 with adult dating site Adult Friend Finder (Ragan, 2016). In this information leak, 414.2 million accounts were compromised. In both of these examples, users of both services were subject to their payment information being released, along with potentially their email addresses, phone numbers, and even physical home addresses. These examples show that the law exists as a means of incentivising good information security practices, but cannot physically stop every attack. That can only be done with proper security training and good practice.

Minimum Privacy Safeguards

The first privacy safeguard I would recommend is two-factor authentication, which would allow a user to ensure that no one other than themself was logging into their account. This is frequently done by sending a text message to the owner of the account, which contains a code that needs to be entered to verify ownership of the account (Authy, 2021). If two-factor authentication is not offered by the organization, then I would recommend implementing it as soon as possible.

In order to protect customer information as much as possible, the second safeguard I would recommend is increasing employee training regarding phishing scams and other forms of social engineering attacks. Using phishing emails is one of the most popular forms of social engineering, and has proven to be an effective method of siphoning customer information (FTC.gov, 2021). Therefore, I believe that training against these kinds of scams is the best way to avoid them.

Decision for the Organization

Regarding the organization’s plan to begin sending customer information to a partnered health monitoring organization, my decision would be to advise against it. Looking at the financial outlook document shows that most consumers say they feel uncomfortable with their data being collected, even if it is anonymous. The first pie chart shows that only about 50% of consumers feel comfortable sharing their data at all, while only 32% of consumers feel comfortable sharing their data in exchange for a discounted rate. While the profitability of the organization is a major concern for any business driver, when the question of ethics comes into play, profitability should take a backseat in favor of increasing favorability with the consumer. When a large majority of consumers say that they are uncomfortable with a proposed idea, the best thing for the company to do is listen to the consumer to protect against lost sales.

References

Authy. (2021). *What Is Two-Factor Authentication (2FA)?* Authy. https://authy.com/what-is-2fa/.

FTC.gov. (2021, May 11). *How To Recognize and Avoid Phishing Scams*. Consumer Information. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

Ragan, S. (2016, October 18). *Researcher says Adult Friend Finder vulnerable to file inclusion vulnerabilities*. CSO Online. https://www.csoonline.com/article/3132533/researcher-says-adult-friend-finder-vulnerable-to-file-inclusion-vulnerabilities.html.

Swinhoe, D. (2021, January 8). *The 15 biggest data breaches of the 21st century*. CSO Online. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Zynga. (2019, September 12). *Player Security Announcement*. Zynga Inc. https://investor.zynga.com/news-releases/news-release-details/player-security-announcement.