Company Case Study-Data Breach

By Tianwei Mo
z5305298

Background

With the development of networks and technology, more and more people store data and privacy in electronic devices and cloud drives. At the same time, more and more powerful software needs all kinds of data from users. Society is experiencing an era of big data where data security becomes more and more important.
However, the problems of data breaches keep emerging. According to the Identity Theft Resource Center's 2021 Data Breach Report, there were 1862 data leaks in 2021, which is 68% more than the number of cases in 2020. These data leakage incidents not only bring property and reputation losses to enterprises but also expose consumers' personal information and privacy.
Alibaba is a business group that has Taobao, one of the biggest online shopping platforms in China, and Alibaba Cloud, a cloud computing service. The company seems to have poor user data management. In 2019, Alibaba cloud divulges the registration information of users to a third-party cooperative company without the user's consent. An employee of Alibaba Cloud took advantage of his work to obtain customer contact information privately and disclosed it to a third-party employee, thus causing customer complaints. Alibaba admitted that the incident was true. The employee's behavior violated the network security law of the people's Republic of China. Apart from that, since November 2019, a graduate had scraped users' information on Taobao for up to eight months and stole more than 1.2 billion user information Before Alibaba noticed. While the criminal earned about 70 thousand dollars from the data, many users were scammed because of data leakage.

Ethical discussion

First, we will talk about the relationship between users' privacy and user information. According to AICPA/CICA, personal information is defined as "information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual" (AICPA/CICA, 2009). Almost all the information user stored online is personal information. From the view of users, data leakage means their rights to privacy have been unethically violated. Individuals have the right to decide what information to disclose and what information to keep private. Based on the consequences that users whose contact information was leaked are harassed by spam phone calls and emails, protecting personal information is moral and necessary.
When considering Alibaba Group as one of the stakeholders, they make profits through

user data. Alibaba Cloud sells cloud drives space and servers to earn money, where user put their data in. Meanwhile, they require a huge amount of user data for cloud computing analysis and development. Data security is of importance to them. Besides, Taobao offers a trading platform where trader information is necessary for transactions. At the same time, data breaches will damage Alibaba's reputation, thus doing harm to the company's business. According to Mill's teleology, to continue the business and earn money, Alibaba has to keep user data in a secure way. Besides, the premise of users using Alibaba's products is the company to protect user data security. Referring to Kant's second formulation of the categorical imperative, it is immoral if Alibaba treats its clients as a mere means to make money. It is not humane to disclose users' information without their agreement. Moreover, according to the ACM Code of Ethics and Professional Conduct, a computing professional should respect the privacy of users. A basic goal of computing professionals is to minimize the negative consequences of computing, including threats to health, safety, personal security, and privacy. Therefore, Alibaba has an ethical duty to keep data safe.

Another stakeholder is the government. Government has the responsibility for protecting the rights and interests of citizens. Based on Kant, though Alibaba has no obligation to be supervised by the Chinese government, it is an imperfect duty. The company would be considered ethical if it shows the desire to be supervised by the government and publish its behavior, such as a list of third parties, and the types of information it collected. Besides, collaborating with the government would be considered a virtue of honesty and reason, because sometimes the company is not able to avoid data leakage. Cooperation means more powerful technology and more secure data storage. Thus, it is ethical if Alibaba stays under the government's surveillance.

Conclusion

To conclude, Alibaba is unethical in the case of the Taobao user data breach. First, the leaked data was scraped by a web crawler designed by a graduate, which shows Alibaba does not pay attention to data security. Besides, Alibaba did not notice the data breach until 8 months later. Either their data protection technology is so backward that it cannot play a protective role, or they did not pay attention to users' data privacy. If it is caused by backward technology, Alibaba should notify the situation to users to be considered virtuous. In terms of the case of Alibaba Cloud data leakage, Alibaba is immoral since a worker can disclose important user data. This would make people question the chaotic management of Alibaba's employee management.

Suggestions

One of the possible steps that Alibaba can take is to upgrade its data encryption system or to cooperate with enterprises specializing in network security and data encryption as this is the most direct way to prevent data breaches. In addition, Alibaba better to re-manage its employees. From the deontology, to prevent employees from divulging private data again, Alibaba has a duty to adjust the employee structure and employee authority and manage

more reasonably. Furthermore, another ethical behavior is to promote knowledge of data leakage to the public. According to previous studies (Romanosky, Telang & Acquisti, 2011) (Solove, & Citron, 2017), though current law on data breaches has some effect, it is difficult to define and restrict data leakage from the legal level. What is important is the users' awareness of data breaches. Only when people consciously protect their privacy on the Internet can the problem of data breaches be alleviated. Considering this as goodwill, Alibaba has the responsibility to do this. As aforementioned, an effective way to prevent data leakage is to stay under the government's surveillance and actively publish its behavior to the public and the government to be virtuous. Specific acts can be giving out a list of data they collect and allowing government intervention and inspection.

Reference

AICPA/CICA. (2009). Records Management: Integrating Privacy Using Generally Accepted Privacy Principles

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. Journal Of Policy Analysis And Management, 30(2), 256-286. doi: 10.1002/pam.20567

Solove, D. J., & Citron, D. K. (2017). Risk and anxiety: A theory of data-breach harms. Tex. L. Rev., 96, 737.