Data Gathering and Privacy Issues

Student Full Name

Institutional Affiliation

Course Full Title

Instructor Full Name

Due date

Data Gathering and Privacy Issues

The specific problem to be addressed by this study is the tendency of data gathering and research to create privacy issues. Forty percent of the two thousand Americans surveyed do not trust companies to use their data from an ethical point of view (Whitney, 2021). The foundation of modern businesses' functioning is confidential information of many sorts, varying from personnel records to client databases. Companies currently collect enormous quantities of client data with the assistance of technology. However, they are generally opaque about the information they acquire and frequently resell, leaving their users apprehensive. Although this technique may provide companies with a competitive advantage in the near term, it lowers customer loyalty and hampers competitiveness in the long run.

Privacy issues have been reported frequently enough in recent years to make users worry if corporations have the necessary means to secure consumer information. Data loss results can be devastating, and many businesses fail to develop adequate plans for worst-case scenarios. The negative consequences of disclosures include unapproved access whether because of data privacy violations or data leakage sharing with other firms that the consumer is unaware of, which could lead to identity fraud or other data abuses (Wieringa et al., 2021). A personal information breach may cause physical, material, or non-material harm to individuals, such as loss of control over their sensitive information, discrimination, fraud, economic loss, reputational damage, or any other substantial economic or social damage, if not addressed appropriately and promptly.

This study's theory is Restricted Access/Limited Control (RALC). Tavani's Restricted Access/Limited Control (RALC) theory defines privacy "in terms of protection from intrusion and information gathering by others (through situations or zones that are established to restrictaccess), not in terms of control over information" (Hugl, 2010, p. 248). Companies are not concerned whether they may control the information provided by their customers merely for their purposes (such as targeted advertising, improving products, predicting sales trends), as long as they implement confidentiality for customers to prevent their personal data disclosure. Companies that take the lead on the privacy issue—by proving that they consider what customers are saying and reacting to their claims—will be firmly positioned to reap the long-term advantages of accessibility to consumer data (Whitney, 2021). The right approach to this strategy involves creating and maintaining the balance between policies and profits.

Peer-reviewed studies that call for further research explain that despite many research efforts on safeguarding sensitive information from being leaked, privacy remains an active research problem (Cheng et al., 2017). This paper highlights companies' data breach risks, systematizes information leakage detection and prevention solutions, and identifies future research possibilities in this field. Another study reveals that the main causes are lack of authentication, misuse of various keys (e.g., regular user and superuser keys) in authentication, or misconfiguration of user permissions in the authorization are the root causes (Zuo et al., 2019, para. 3). This research investigates why such significant leaks occur and what tools can be used to identify them automatically. Mobile apps from the Google Play Store susceptible to data leak attacks were also evaluated. The last peer-reviewed study examined big data techniques' ethical, security, privacy, and operational challenges and the potential reputational damages to businesses (Ogbuke et al., 2020, par. 1). The research provides a comprehensive review of the use of big

data in the management of supply chains and the advantages it offers to both businesses and society.

References

Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *11*(3), 528–542. https://doi.org/10.1002/widm.1211

Hugl, Ulrike. (2010). "Approaching the value of privacy: Review of theoretical privacy concepts and aspects of privacy management" *AMCIS 2010 Proceedings*. 248.

Ogbuke, N. J., Yusuf, Y. Y., Dharma, K., & Mercangoz, B. A. (2020). Big data supply chain analytics: Ethical, privacy and security challenges posed to business, industries and society. *Production Planning & Control*, *33*(2-3), 123–137. https://doi.org/10.1080/09537287.2020.1810764

Whitney, L. (2021, August 17). Data privacy is a growing concern for more consumers. *TechRepublic.* https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/

Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2021). Data analytics in a privacy-concerned world. *Journal of Business Research*, 122, 915–925. https://doi.org/10.1016/j.jbusres.2019.05.005

Zuo, C., Lin, Z., & Zhang, Y. (2019). Why does your data leak? Uncovering the data leakage in cloud from mobile apps. *2019 IEEE Symposium on Security and Privacy (SP)*, 1296–1310. https://doi.org/10.1109/sp.2019.00009