Title: Companies should be responsible for Users Data Privacy as the Users are purchasing their services

By: Cyrus Tan Chin Xiong 23100076

In the Digital Landscape of today's time, a majority, if not all, of companies in the world utilizes the data information of its users in a unique way. By using the data with the agreement of users, the users expect robust data protection as they willingly providing their information to the companies to use their product and services along with protection for their personal data. This expectation places significant legal and ethical responsibilities on the companies to ensure that data privacy is an integral part of their corporate operations.

In the journal *Building Trust in Fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust,* Aldboush and Ferdous (2023), they explore this responsibility in the context of Financial Technologies, Fintech. They argue that as Fintech companies rely increasingly on big amounts of data and artificial intelligence to provide users a personalized service, they must also address the ethical issues these technologies present, such as data privacy and transparency. The authors highlight that the consumers trust hinges on the companies' ability to protect the user's data, recommending practices like data encryption, user consent, and having clear communication about the data usage. These measures not only ensure compliance with data protection laws but also establish trust, essential for a long-term relationship with users (Aldboush & Ferdous, 2023).

Similarly in *Corporate Social Responsibility, Data Protection and the Right to Privacy*, Steele (2022), he has emphasised that data protection has become a critical aspect of corporate social responsibility. Steele notes that with regulations such as General Data Protection Regulation, companies must now consider data protection as an obligation to their users. The journal underlines that data protection is not only a regulatory requirement but an essential part of consumer rights. For companies providing paid services, strong responsibility to data privacy reinforces trust and improves reputation. Steele's research supports when companies prioritize privacy, they align themselves with ethical standards that support consumer autonomy and the right to privacy (Steele, 2022).

In conclusion, both journals highlight that data privacy is pivotal to building user trust and fulfilling corporate social responsibility. By implementing privacy measures and adhering to ethical guidelines, companies can not only meet legal requirements but also foster positive, trust-based relationships with their users. As data use in services grows, so too will the need for responsible and transparent data practices that protect consumer rights.

[398 Words]

References

- Aldboush, H. H. H., & Ferdous, M. (2023). Building Trust in Fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. *International Journal of Financial Studies*, *11*(3), 90. https://doi.org/10.3390/ijfs11030090
- Steele, V. (2022). Corporate social responsibility, data protection and the right to privacy. *openjournals.ljmu.ac.uk*. https://doi.org/10.24377/LJMU.SLJ.vol2article577

A Response on the Selected Articles Concerning User Responsibility the Key to Data Privacy and Technology Companies Burden of privacy

By Tan Jia Liang

This response examines the balance of the responsibilities of users and technology companies in maintaining data privacy. In an era where the value of personal information is increasing. Users are often provided with privacy settings to manage their data. However, the complexity and structure of these settings often harms users. This analysis explores the role of user control and the responsibility of technology companies to prioritize user privacy. Although users have access to privacy settings, but responsibility for data privacy should rest with technology companies that have the expertise to build secure systems by default.

First article by Saura et al. (2021) discuss the concept of "Privacy by default" within Social Internet of Things (SIoT) networks, emphasizing that although users can technically control it, but many people still lack the knowledge to fully protect their data. This leads to extensive data collection that users may not fully understand. This highlights a key problem: Users are inevitably responsible for managing complex privacy settings without adequate support or transparency. I found Saura et al.'s arguments interesting. This is because it emphasizes the hidden burden of users. and recommend that companies have the knowledge and ability to provide stronger basic privacy protections.

Second article by Debatin et al. (2009) discuss user control. Specifically, it examines how Facebook users perceive and interact with their privacy settings. Even though privacy controls can be accessed but users often reduce the risk of sharing information by assuming the default settings are secure. This "privacy paradox" occurs when users continue to share personal information despite privacy concerns. Debatin et al. (2009) shows that the design of privacy settings and user experience affects user behavior. It shows that users do not always act in their best privacy interests. Especially when default settings are involved. The findings reinforce the idea that tech companies should shoulder more responsibility by tightening privacy controls. Easy to use and protected by default.

Both articles support the conclusion that although users can control their privacy settings, tech companies should have primary responsibility for ensuring data privacy. Companies are better equipped to reduce the burden on users by creating secure default settings and simplifying privacy controls. These insights will be valuable in my research on data privacy. especially in supporting industry standards in the future.

(379 words)

References

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2009). Facebook and online privacy: attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). Setting Privacy “by Default” in Social IoT: Theorizing the Challenges and Directions in Big Data Research. Big Data Research, 25, 100245. https://doi.org/10.1016/j.bdr.2021.100245

A Brief Response on Selected Articles Concerning the Responsibility of User and Company on Protecting Data Privacy.

by Pang Wei Sheng

The rapid advancement of technology has brought data privacy to the forefront of modern concerns, highlighting an essential debate: Who's responsible for user data? Should it be companies, or the users themselves? Indeed, some argue that vigilance on the part of users is essential because the public is so unaware about data privacy, but the discussion, based on two important articles, calls on companies above all to bear the responsibility of protecting data privacy in the future. Taking this perspective, users should be cautious, but companies are able to implement stronger guarantees and help build trust.

The first article by Jain et al. (2016) discusses data privacy issues related to big data through privacy preserving techniques k-anonymity, l-diversity and t-closeness. By offering these methods for anonymizing data and user privacy while retaining its analytical value, companies can better safeguard user privacy in the data driven world of today. However, this article does not provide guidance on implementation, there are a lot of challenges involved in these techniques and may leave the readers with an incomplete understanding. Although first published in 2016, this article remains a valuable read for understanding foundational techniques companies can adopt to protect user data. Overall, this article reinforces the argument for corporate accountability in setting and upholding strict data protection standards.

The second article, by Jain, Sahoo, and Kaubiyal (2021), is a comprehensive review of and analysis of security and privacy issues in online social networks (OSNs). They explore on the various privacy threat users faced within online social networks (OSN) such as identity theft, cyberbullying and phishing. In addition, they have offered some ways users can do to have better security on social platform such as adopting a robust password. This article is significant because it explained common threats on OSNs and offer insight to technical challenges and potential solutions. Overall, OSNs is valuable for connectivity but on the other hand expose the users to diverse threats that has to be dealt with by the users and by the company itself to improve the level of security.

In conclusion, companies should bear on the main responsibility because they control privacy settings, security protocols and handling of user data. While users' responsibility remains critical in the growing of digital landscape, companies must view privacy as their ethical obligation to gain user's trust. I plan to use the second articles to better understand on the user's behaviour that cause them to disclose their privacy online. I will look for more articles that would discuss the training of artificial intelligence from users' data with alignment with users' privacy.

[426 words]

References

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex & Intelligent Systems, 7*(4), 2157-2177. https://doi.org/10.1007/s40747-021-00409-7

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: A technological perspective and review. *Journal of Big Data, 3*, Article 25. https://doi.org/10.1186/s40537-016-0059-y