ENG 1044: ENGLISH FOR COMPUTER TECHNOLOGY STUDIES

Coursework 3: Academic Paper

Names	Student ID
1.CYRUS TAN CHIN XIONG	23100076
2.PANG WEI SHENG	24035115
3.TAN JIA LIANG	24035123
4.	

Programme	**ENG 1044: ENGLISH FOR COMPUTER TECHNOLOGY STUDIES**
Tutorial Group	**3**
Title	**From Users to Company: Who is more responsible for handing data?**

Evaluation Form

Assessment Criteria	First Marker	Second Marker
Introduction	/10	/10
Body – Argument	/30	/30
Body – Counter argument & Rebuttal	/15	/15
Conclusion	/10	/10
CONTENT (65 marks)	**/65**	**/65**
LANGUAGE/STYLE	**/15**	**/15**
IN-TEXT CITATIONS, REFERENCE LIST & FORMAT	**/10**	**/10**
ORGANISATION	**/10**	**/10**
TOTAL MARKS 100 marks (40%)	**/100**	**/100**
	/40%	**/40%**
Comments:		

ENG 1044

ENGLISH FOR COMPUTER TECHNOLOGY STUDIES

Title of Research Paper:

From Users to Company: Who is more responsible for handing data?

Group NO.: 3

Prepared by:

1. CYRUS TAN CHIN XIONG

2. PANG WEI SHENG

3. TAN JIA LIANG

Prepared for:

R Lakshmi Priyadarshni

Date of submission:

12th December 2024

1.0 Introduction

The debate over privacy, then, is one of the hottest debates in this digital and cyber communication era. This is so because the way in which people interact with the world and each other has changed much, sharing, and giving information, since the coming of the digital age. The private sphere used to be one of a personal right. The right to privacy now seems to be a matter so complex and very often quite controversial. This raises a basic question: Who is responsible for users' data? Should it be the person who collected or the company that profited from it? The same question becomes very valid in the arena of social media. online service and technology platforms, tracking, storing, and analysing personal data.

Debatin et al. (2009) show how social networking sites, while offering convenience and connectivity, also introduce considerable privacy risks. These platforms are built upon the collection of user data, often without clear consent or full disclosure to users. They therefore argue that the platforms have created a kind of "privacy paradox" in that, although users are concerned about privacy, they usually do not take sufficient steps to protect their information, and companies continue to exploit this gap. Although, users are given some control over their privacy settings, companies should bear the primary responsibility for protecting user data, as they not only manage the features of the platform while also adhering to ethical and legal standards in ensuring transparency and security.

2.0 User’s Control of Features

The reason company must bear the responsibility of protecting user’s data is because the company control the user’s features. For instance, Rivadeneira et al. (2023) discuss how the (Internet of things) IoT systems integrate models that ensure the privacy of users’ data rights into the design of their platforms. They emphasize that companies should have to implement user privacy in the design and by default through strict measures such as data storage in

secure environments and automatic encryption, because user data is automatically protected without the manual intervention by the users. This proactive way puts the burden on the companies to make sure that their operations on privacy are compliant, and data handling is secure by default, which supports the thesis that the companies must handle user's data with care.

Similarly, Debatin et al. (2009) explore the gap between the users' expressed concerns about privacy and their actual behaviours on Facebook. The study shows that users often do not engage with their privacy settings or fully understanding the consequences of their sharing habits. For instance, many Facebook users share their own personal information without adjusting their privacy settings, exposing them to potential data breaches. This shows that even when users are given the power to control their privacy, companies still play a significant role in the protection of user data. For instance, Facebook has been criticized for allowing the users personal data to be exposed despite privacy settings. This shows that user behaviour alone cannot guarantee secure protection in terms of privacy. Therefore, this is one of the reasons that emphasizes companies must take full responsibility concerning data privacy security and ensure that this process is fully transparent on the management of the users' information.

On one other line of reasoning, Saura et al. (2021) emphasizes that privacy should be "by default" in Social IoT systems, where personal information can flow from one device to another interchangeably. They refer to numerous examples, such as smart home devices, which often collect sensitive information in their home without clear user consent or understanding. Saura et al. (2021) argues that companies must establish automatic privacy settings, such as anonymizing user data or restricting data sharing unless explicitly authorized, right from the very beginning. This will ensure that users are not inadvertently exposed to data privacy risks simply because they are unaware of the implications of their device usage.

These studies show that while users should be able to control their privacy settings, the ultimate responsibility for ensuring user data protection lies with the companies. Companies can embed privacy by design, ensure transparency, and uphold ethical and legal standards to create a secure digital environment where users can be confident their data is safe.

3.0 **Users are paying for their data's protection**

The protection of data is the companies' responsibilities because the users are paying the company money to use their services and are expecting their data to be securely protected. It becomes an important corporate responsibility for any company in the digital economy, where the users are paying customers. This is much broader than mere legal compliance, ethical and trust-building actions go hand in hand with privacy. The combined understanding from Aldboush & Ferdous (2023), Steele (2022), and Gellert & Gutwirth (2017) points out that it is needed to integrate strong data protection measures into organizational functions to meet user expectations and uphold social norms.

Aldboush and Ferdous (2023) highlight that big data and artificial intelligence play a significant role in service delivery in fintech services. They add that customers share sensitive data with confidence that it will be well protected and used transparently. They recommend that this will require the encryption of information, clear mechanisms of consent, and transparency in the use of data. These are not just some legal requirements but also cornerstones in customer relationships. When companies fail to ensure the protection of user data, they automatically undermine the trust that sustains long-term engagement, with consequences that are particularly serious in sectors like fintech, where personal data is integral to service personalization.

Steele (2022) drives this argument further by framing data protection within the broader concept of corporate social responsibility. According to Steele (2022), regulations like the

General Data Protection Regulation (GDPR) set a floor minimum, but to meet ethical expectations companies need to go far beyond the floor instead of just meeting it. Consumers think that data privacy, especially for paid services, as a part of what they are buying. Not only must companies abide by laws, but they also need to show that they can live up to the ethical principles. This alignment creates brand loyalty within consumers and strengthens reputation. For businesses, data protection in their Corporate Social Responsibility (CSR) policy means regard for customer rights and a plus to their own brand image, placing them above other business competitors that would rather treat privacy as just a formality.

Gellert and Gutwirth (2017) have added a legal perspective, pointing out that even though privacy laws are influential in forming corporate responsibilities, they are just one side of the coin. The authors say that at times, social expectations surpass legal requirements, especially when consumers are paying for some services. Users view data breaches not only as technical failures but also as breaches of trust placed in them by the company. This is where the concept of 'privacy by design' fits in. As emphasized in the research shown, the companies service architecture needs to have privacy measures developed into them the start. This also makes sure that the protection of data is treated as an important and fundamental function of the service, reminding them that privacy is not something that is an addition to the service, but an important and major service provided when the users pay for it.

Data privacy in paid services is a multidimensional responsibility, bringing together legal compliance, ethical consideration, and customer trust. Companies must make sure that proper privacy is granted to all users, not only because it is demanded by the law but also for ethical reasons. As Aldboush & Ferdous (2023), Steele (2022), and Gellert & Gutwirth (2017) propose, taking care of data protection will increase trust, improve brand reputation, and secure long-term relations with clients. In a data-driven world, responsible and transparent data practices are essential for long-term corporate success.

4.0 Counterargument/Rebuttal

Although the articles discussed previously agrees that the companies must bear the burden of the users' privacy, but the users also play a crucial role for their privacy because they have the knowledge and tools to protect themselves. As a substantial number of users keeps growing in the digital world, in platforms such as social media. The statistics shows that family applications of the meta company which includes applications such as Instagram, Facebook and WhatsApp reached its daily amount of active people which amounts to around 3.29 billion people on average in September 2024. Noted within INVESTOR RELATIONS, it is stated that it is easy for attackers to search for suitable people to attack from the huge mass of users in social media, from the information that the users willingly shared within social media. Jain et al. (2021) stated that the personal data shared by users can be exploited by attackers with methods such as phishing, which is implemented by obtaining sensitive information through fake websites or messages. For companies it is difficult to monitor in real time about these threats as the different variation and spread of these threats is easier within social media.

On the other hand, this shows the users lacking awareness and them putting too much trust on these platforms. Jain et al. (2021) highlights some guidelines for users to secure their own privacy on these platforms, which are becoming more important when online social media platforms and networks have become an integral part of everyone's life. First, the users should choose a strong password which contains at least 8 letters with numbers and symbols mixed within, and users should not use the same password for all their accounts. Second, users should be careful on what they share, as some users directly or indirectly write their personal information in their posts. Third, users should avoid sharing their current locations, being unable to do this may allow users to be targeted by attackers allowing them to easily commit crimes such as robbery in their real life if they know where you are and what you are doing at the time. Lastly, users should avoid adding too many people in their social media, such as only adding friends that you are familiar in real life, adding random people increases the risk

of being attacked and receiving spam if the users information are being exposed to many other random users, and users should set their profile to private so which their information cannot be seen by stranger.

However, not all users possess the knowledge or skills to effectively manage their privacy. From the point discussed above, although users also have some responsibility in their privacy, some of them do not have the knowledge or skills to effectively manage their privacy, and companies collect all the user's data and provide services to users. From the perspective of users, although they can minimise the risk from data breaches by taking security measures and adjust privacy settings, they cannot avoid companies breaching their data because of the vulnerability of the system or third parties that intend to do that. Internet Society. (2019) stated that companies have the responsibility to provide transparency of privacy policies and information, as to make it easier for users to understand how companies collect and use the data of the users. On another note, it also agreed that companies must implement robust security measures to protect user data from unauthorized access, breaches, and potential misuse because not all users have the knowledge and awareness to take awareness to care of their privacy.

5.0 **Conclusion**

In conclusion, while users have a significant role to play in the protection of their privacy, the ultimate responsibility lies with the companies that collect and manage the information. As argued above, companies must incorporate efficient privacy mechanisms at the design stages of their platforms, ensuring transparency, encryption of data, and adherence to legal and ethical standards. Though users might have some control over their privacy settings, very few people really know how to protect their information or understand the associated risks. Apart from this, companies must also listen to their users so that they can design a more user-friendly platform. The responsibility rests with businesses in terms of creating a secure

environment that respects user privacy, especially in paid services, where consumers expect both legal compliance and ethical data handling.

What it means is that individual users can only help protect their data through prudent behaviour and awareness, but it stays a business obligation to exercise effective and clear data protection. Moving ahead, companies will have to embrace the spirit of trust and ethics for data privacy, which, in addition to meeting the requirement of law, will only forge lasting relationships with customers. In the digital age, privacy is not an add-on; it is more of a service that must be put in the foremost priority for the safety and security of the data provided by the users.

(2127 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

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

Internet Society. (2019, July 2). Principles for responsible data handling. Retrieved November 22, 2024, from https://www.internetsociety.org/policybriefs/responsible-data-handling/

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*(1), Article 25. https://doi.org/10.1186/s40537-016-0059-y

Micah Altman, Alexandra Wood, David R O'Brien, Urs Gasser, Practical approaches to big data privacy over time, *International Data Privacy Law*, Volume 8, Issue 1, February 2018, Pages 29–51, https://doi.org/10.1093/idpl/ipx027

Rivadeneira, J. E., Silva, J. S., Colomo-Palacios, R., Rodrigues, A., & Boavida, F. (2023). User-centric privacy preserving models for a new era of the Internet of Things. *Journal of Network and Computer Applications*, *217*, 103695. https://doi.org/10.1016/j.jnca.2023.103695

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

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