**Frontiers in Business, Economics and Management**
ISSN: 2766-824X | Vol. 11, No. 1, 2023

# Ethical Challenges of Data Commingling in Business

**Lujie Wang**[1, *]

[1] Department of Marketing, The University of Queensland, Queensland, Australia
[*] Corresponding author: Lujie Wang (Email: lujie.wang@uqconnect.edu.au)

**Abstract:** Data commingling involves merging data from various sources into a shared infrastructure. However, this poses ethical challenges for businesses. This article delves into the ethical issues that arise from data commingling and its impact on organizations. It also provides recommendations for responsible data management. Real-world cases, such as LinkedIn's data handling, highlight the consequences of data commingling on customer trust and company credibility. To overcome these challenges, businesses should explore the creation of multi-cloud data lakes, offer employee training, and advocate for global regulations on data commingling.

**Keywords:** Data commingling, Ethics, Management, Privacy, Security.

## 1. Introduction

Data plays a crucial role in today's digital era for businesses. With technology advancements, the significance of data has increased, but this has also raised concerns regarding data privacy and misuse. Data commingling, which involves merging information from various sources within a shared infrastructure, has become widespread in business. This article explores the ethical dilemmas linked to data commingling and its impact on organizations. Through real-world case studies, such as LinkedIn's data practices, we aim to highlight the effects of data commingling on customer trust and company credibility. We will also provide recommendations for responsible data management to address these challenges.

### 1.1. What is Data Commingling

With the development of technology, people understand more about the importance of data. Besides, data privacy protection has become a topic of concern, and data misuse is one of the most common privacy problems in business. Commingled data is information stored in a shared infrastructure, such as multiple related or connected databases (Commingled, 2016). In this essay, I will discuss how data commingling may cause ethical issues in the business place and the impact on the organization by analyzing a real-world case example.

### 1.2. Why data commingling important to business?

Sophisticated use of consumer data allows for personalized product offering and let marketers pass along additional benefits to consumers as they can operate more efficiently with information (Martin & Murphy, 2017). However, commingling happens when an organization captures data from a specific audience for a specific stated purpose, then reuses that same personal data for a separate task in the future (Invisibly, 2021). Because of the potentially vast benefits of customer data, fewer companies have systematically considered the ethical aspects of data management, which could have broad ramifications and responsibility (Edquist et al., 2022). So, at the enterprise level, avoiding data commingling is suitable for long-term business development.

### 1.3. How is Commingling useful?

The growth of technology has also offered the expansion of linkable data resources, especially in social media platforms (Soussan & Trovati, 2021). Using stored customer data in other business activities allows the company to save the cost of collecting information and the time cost, so commingling is a profitable choice for companies. Besides, only 60 percent of consumers are aware that their information has been compromised (Ablon et al., 2016). The difficulty of traceability has led many businesses to believe that commingling is an opportunistic method for profit-making.

### 1.4. What are the ethical issues with Data commingling?

There are three possible causes of ethical problems. The first is the original company that improperly stores customer information. Many organizations make the mistake of commingling data with different sensitivities (Somani, 2020) which means that once a company merges 500 gigabytes of sensitive data into a data lake containing 10 terabytes of public data, they must shoulder the responsibility to secure all 10.5 terabytes of data. However, most companies will think more about their own interests than about the ethical issues of whether they will harm their customers.

The second is a company that has accidentally used commingling data. The ethical issue that arises here is that these companies have not bothered to trace the origin of this information. the main problem is employees' training as their behavior is fixed, they may not have paid attention to how the information was obtained.

The third is companies that deliberately take commingling data for profit. This is the most serious ethical issue, as these companies continue to exploit the loopholes in the law by using commingling data, knowing that it will be harmful to their customers.

### 1.5. Security as a business enabler

Industry reliance on data has grown exponentially in the present dynamic and highly competitive, challenging business environment (Mubarak Alharbi et al., 2013). The focus of competition has also risen from how to obtain effective information to how to obtain information ethically. As more and more famous companies are exposed to the

problem of commingling such as LinkedIn, Facebook, and so on (Hill & Swinhoe, 2022), consumers are also paying more attention to the security of their information. If other companies can access their own customers' information, it will also lead to a decline in customer trust and a loss in credibility. Therefore, improving the company's safety factor is also a way to combat commingling. If companies can properly store the collected customer information and avoid commingling will be a new challenge in data security.

### 1.6. Long-term impacts - company loses credibility

As personal data has become a new source of economic value which is extremely useful for advertising (Esteve, 2017). In the short term, companies may think that this is a cost-effective and fast way to access customer information through commingling, but this is not conducive to long-term business success. Research shows that loyalty program customers significantly reduce their trust in the organization after a data breach crisis (Chen & Jai, 2021). Therefore, if companies are seeking long-term development, it is essential to maintain relationships with customers and ethical management of customer data is undoubtedly the key to increasing customer trust. Because commingling issues are not easily detected and are difficult to trace back to the source, if companies can ethically avoid using this data, it can create strong brand equity as technology evolves and customers trust it. Therefore, if companies are only interested in the immediate profit by using commingling data will be eliminated in the end.

### 1.7. Case in Focus: LinkedIn

DPC, in 2017 found out that LinkedIn was using people's email addresses – some 18 million in all – in a way that was not transparent, in a bid to get people to sign up for the service and then using in a hashed form for targeted advertisements on the Facebook platform (Lunden, 2018). However, the DPC does not solve the problem as we still do not know where LinkedIn got the 18 million email addresses and other relevant data. LinkedIn was not fined in the process - which may have been a lever that prompted the company to act from the outset rather than changing its approach after it was called out - because the regulator did not have the power to enforce the fine.

This case shows us that the impact of commingling is enormous and that customers need to know when their information, registered at an unknown time, will be used. Besides, there is a problem with data commingling. In that case, there must be more than one company to take responsibility, so this example shows us that companies need to be vigilant not only about the source of customer information but also about the information security of their own company.

Moreover, there is no doubt that LinkedIn is abusing commingled data, and from the enormous data, we can see the seriousness of the problem. However, based on the DPC's solutions, many regulations and policies still need to be improved for data commingling. Nevertheless, judging from the fact that more and more companies are exposed, this is not a loophole that companies can exploit, and as the law improves, the punishment will be more serious.

### 1.8. Recommendations

Build and maintain multi-cloud data lake

I recommend that the company can build up a multi-Cloud data lake that proposes using combined cloud services from different providers (Zagan & Danubianu, 2021). This method is to help the company solve the problem of data commingling from the source. Although it may require greater technical skills to achieve communication between each platform, it also means that the company can be benefiting from the advantages of each platform. Using a multi-cloud data lake allows the company to store consumer data based on different sensitivities which can reduce the possibility of data commingling.

Train employees how to avoid data commingling

Many companies attach great importance to the privacy of customer information, but due to inadequate training of employees, ethical issues of misuse of sensitive information are prone to arise. The most important thing is to solve employees' behavioral issues of ISA (information security awareness) through regular training (Bulgurcu et al., 2010). This can help companies increase employee sensitivity to customer information acquisition, thereby reducing the probability of data commingling.

Establish global regulations of data commingling

As more and more companies rely on personalized customer information to achieve marketing success, they will prefer self-regulation to stay ahead in a rapidly changing environment (Sarathy & Robertson, 2003). Thus, every country needs to use harsh measures, setting the same standards and penalties for companies. Besides, soft law should also be used, like the reactions of disappointed customers, primarily when those reactions are spread by social media, which often be more effective than mere fines or penalties (Lee et al., 2016). Nevertheless, whether it is a strict policy or a soft law, the most important thing is to ensure consistency and to give companies a level playing field.

## 2. Conclusion

As data privacy increasingly becomes a critical societal concern, the issue of data comingling is also getting more and more attention (Li et al., 2023). Whether companies can manage data ethically will become an opportunity and a challenge. The implementation of ethical management requires the company to have strict supervision, not only to track the information but also the protection of its company's data security. Therefore, companies must build a multi-cloud data lake and train employees to prevent commingling. Furthermore, establishing global regulations is also vital to create a fair competition environment.

## Acknowledgment

This article was solely authored by Lujie Wang, who came up with the research idea, conducted a literature review, gathered and analyzed data, and wrote the manuscript. All aspects of the research, such as conceptualization, methodology, data interpretation, and conclusions, were done solely by Lujie Wang. Lujie Wang has approved the final manuscript for submission.

## References

[1] Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. (2016). Consumer attitudes toward data breach notifications and loss of personal information. RAND.

[2] Bulgurcu, Cavusoglu, & Benbasat. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS*

*Quarterly: Management Information Systems*, *34*(3), 523. https://doi.org/10.2307/25750690

[3] Chen, H. S., & Jai, T.-M. (catherine). (2021). Trust fall: data breach perceptions from loyalty and non-loyalty customers. *Service Industries Journal*, *41*(13–14), 947–963. https://doi.org/10.1080/02642069.2019.1603296

[4] *Commingled*. (2016, January 18). Insightsoftware. https://insightsoftware.com/encyclopedia/commingled/

[5] Edquist, A., Grennan, L., Griffiths, S., & Rowshankish, K. (2022, September 23). *Data ethics: What it means and what it takes*. Mckinsey.com; McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes

[6] Esteve, A. (2017). The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law*, *7*(1), 36–47. https://doi.org/10.1093/idpl/ipw026

[7] Hill, M., & Swinhoe, D. (2022, November 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

[8] Invisibly. (2021, August 6). *7 Examples of Data Misuse in the modern world*. Invisibly. https://www.invisibly.com/learn-blog/data-misuse-7-examples/

[9] Lee, W. W., Zankl, W., & Chang, H. (2016). An Ethical Approach to Data Privacy Protection. *ISACA*, *6*. https://redi.anii.org.uy/jspui/bitstream/20.500.12381/441/1/An-Ethical-Approach-to-Data-Privacy-Protection_joa_Eng_1216.pdf

[10] Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., Liu, X., & He, B. (2023). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*, *35*(4), 3347–3366. https://doi.org/10.1109/tkde.2021.3124599

[11] Lunden, I. (2018, November 24). LinkedIn violated data protection by using 18M email addresses of non-members to buy targeted ads on Facebook. *TechCrunch*. https://techcrunch.com/2018/11/24/linkedin-ireland-data-protection/

[12] Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

[13] Mubarak Alharbi, I., Zyngier, S., & Hodkinson, C. (2013). Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce. *Journal of Enterprise Information Management*, *26*(6), 702–718. https://doi.org/10.1108/jeim-07-2013-0039

[14] Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics*, *46*(2), 111–126. https://doi.org/10.1023/a:1025001627419

[15] Somani, A. (2020, January 9). *Preventing data from becoming A liability*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/01/09/preventing-data-from-becoming-a-liability/?sh=3be50e2a2f85

[16] Soussan, T., & Trovati, M. (2021). Social Media Data Misuse. In *Preprints*. https://doi.org/10.20944/preprints202103.0331.v2

[17] Zagan, E., & Danubianu, M. (2021). Cloud DATA LAKE: The new trend of data storage. 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA).