Analysis of the 2019 Facebook Data Breach Case Study

Ritesh Kumar

2024SP_MS_DSP_485-DL_SEC61: Data Governance, Ethics, and Law

Module 4

Data Governance Case Study 2

Candice Bradley and Pushkar Shah

July 8, 2024

Table of Contents

The Data

The data for this case study primarily stems from an investigation by UpGuard, a cybersecurity firm, which discovered two databases on Amazon's publicly accessible S3 cloud service. These databases belonged to Cultura Colectiva, a Mexican media company, and a Facebook-integrated app called At the Pool. The authors[1,2,3] clearly explain how the data were collected by detailing the discovery process, including attempts to contact the responsible parties and the subsequent involvement of Amazon Web Services (AWS) and Bloomberg. In the authors' view, the data collection and analysis are adequate as they thoroughly trace the steps taken to uncover and address the breach. They highlight the sheer volume and sensitivity of the leaked data, providing a comprehensive overview of the breach's implications.

Relevance to Data Governance

The problem of the 2019 Facebook data breach fits into a data governance framework primarily as a management and ethical issue. From a management perspective, the breach underscores the need for robust data protection policies and the proper handling of user data by both Facebook and third-party developers. Ethically, it raises questions about the responsibility of companies to protect user information and maintain transparency regarding data breaches. The case highlights the failures in data governance practices at multiple levels, including inadequate response times and insufficient user notification, which ultimately undermine trust and accountability.

Relevant Legislation

The case study references several pieces of relevant legislation, including the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA)

in the United States. GDPR mandates stringent data protection measures and requires companies to notify users promptly in the event of a data breach. The CCPA grants California residents the right to know what personal data is being collected, how it is being used, and with whom it is being shared. These regulations are highly relevant as they aim to enforce better data security practices and ensure greater transparency. The case study suggests that such legislative frameworks are crucial in holding companies accountable and protecting consumer data.

If no legislation is mentioned, the authors suggest a need for comprehensive data protection laws that mandate transparent communication from companies in the event of a breach. They argue for regulations that ensure companies like Facebook are proactive in protecting user data and provide clear guidelines for breach notifications and data handling practices. The authors advocate for a balanced approach that includes both regulatory oversight and corporate responsibility to safeguard personal information.

Data Governance Solution

The key takeaway from this case study is the critical importance of robust data governance practices to prevent data breaches and maintain user trust. The authors suggest that companies need to implement stringent data protection measures, conduct regular security audits, and ensure transparent communication with users regarding data breaches. Existing solutions, such as GDPR and CCPA, are steps in the right direction but may not be fully adequate due to varying enforcement levels and the evolving nature of cyber threats.

Additional solutions could include:

1. Enhanced Security Protocols: Companies should adopt advanced encryption methods, regularly update security protocols, and conduct comprehensive vulnerability assessments.

2. User Education and Awareness: Increasing user awareness about data privacy and security practices can empower individuals to take proactive steps in protecting their personal information.
3. Cross-industry Collaboration: Encouraging collaboration between technology companies, cybersecurity experts, and regulatory bodies can foster the development of more effective data protection strategies.
4. Continuous Monitoring and Improvement: Establishing a culture of continuous monitoring and improvement within organizations can help identify and mitigate potential security risks before they lead to breaches.

In summary, the Facebook data breach case study underscores the need for robust data governance frameworks that integrate management, legal, and ethical considerations. By implementing comprehensive data protection measures and ensuring transparent communication, companies can better safeguard user data and maintain public trust.

References

1. [1]Newman, Lily Hay. “What Really Caused Facebook’s 500M-User Data Leak?” *WIRED*, April 6, 2021. https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/.
2. [2]Ho, Foo Nin, Nga Ho-Dac, and J. Sonia Huang. “The Effects of Privacy and Data Breaches on Consumers’ Online Self-Disclosure, Protection Behavior, and Message Valence.” *SAGE Open* 13, no. 3 (July 1, 2023). https://doi.org/10.1177/21582440231181395.
3. [3]Lulandala, Emmanuel Elioth. “Facebook Data Breach: A Systematic Review of Its Consequences on Consumers’ Behaviour Towards Advertising.” In Asset Analytics, 45–68, 2020. https://doi.org/10.1007/978-981-15-3647-2_5.