Borneo International Journal eISSN 2636-9826; Vol.8 (4); 2025; 35-41
Published by *Majmuah Enterprise*
www.majmuah.com

Data Privacy and Misuse of Personal Information

NUR SABRINA MOHD SHAFAWI, MOHAMAD FADLI BIN ZOLKIPLI

School of Computing, College of Arts and Science, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: nursabrinams06@email.com, m.fadli.zolkipli@uum.edu.my | Tel: +60166871636 | +60177247779 |

Received: November 17, 2025
Accepted: November 25, 2025
Online Published: December 01, 2025

Abstract

In the age of digital communication, social media platforms have revolutionised the methods by which individuals share, communicate, and express themselves online. Nonetheless, this simplicity also increased the risks of data privacy infringements and the exploitation of personal information. This article investigates the growing concern of data exploitation on social media platforms, highlighting the methods of user data collection, analysis, and possible misuse for economic, political, or nefarious objectives. The research examines the ethical, legal, and technological difficulties related to personal data protection through an analysis of academic literature, case studies, and privacy breach reports. Frameworks such as GDPR and Malaysia's PDPA are utilised to evaluate privacy threats and user behaviour. It also examines existing preventative measures, like privacy settings, awareness campaigns, and platform accountability, while predicting future risks that stem from AI-driven profiling and cross-platform reconnaissance. The results highlight severe inadequacies in enforcement, user comprehension, and ethical platform design. The article concludes by recommending measures to improve user knowledge, fortify governance, and advocate ethical data practices on social media platforms.

Keywords: data privacy; personal information misuse; cybersecurity

1. Introduction

In the digital era, personal data has emerged as a valuable asset, gathered, analysed, and commercialised by social media platforms, advertising, and third-party organisations. Although social media promotes worldwide connectedness and self-expression, it also subjects users to considerable privacy threats. The extensive dissemination of personal information, sometimes under ambiguous terms of service, has resulted in increasing apprehensions over unauthorised data collection, behavioural profiling, and identity exploitation (Gruzd et al., 2020; Shin, 2020). The issue of data privacy becomes particularly pressing in regions such as Southeast Asia, where digital use is rapidly increasing, while legislative enforcement is ineffective (Hamzah et al., 2018; Fernando et al., 2025). The Personal Data Protection Act (PDPA) was enacted in Malaysia to protect user information, yet issues remain regarding ensuring compliance among e-commerce platforms and social media services (Ali et al., 2025). Prominent breaches and instances of data exploitation, exemplified by the Cambridge Analytica scandal, have underscored the ethical and legal deficiencies in existing data governance frameworks (Boldyreva et al., 2018).

The paper addresses the exploitation of personal data on social media platforms, emphasising privacy risks, legal frameworks, and user awareness. It utilises a varied corpus of literature, including empirical studies, legal analyses, and case-based research, to identify patterns of data exploitation and assess existing preventive measures. The study examines future concerns, including AI-driven profiling and cross-platform monitoring, which confound conventional concepts of consent and control (Tufekci, 2021; Zhang et al., 2022). This paper seeks to outline the progression of data privacy issues by analysing worldwide patterns with Malaysian-specific situations, evaluate the efficacy of current legal and technical regulations, and provide pragmatic solutions for consumers, developers, and legislators. The study enhances comprehension of the commercialisation and contestation of personal data within the digital public world.

2. Literature Review

2.1 Evolution of Data Privacy Concepts

The concept of data privacy has evolved significantly over the past century, shaped by technological advancements, legal milestones, and shifting societal expectations. Initially rooted in the right to be left alone, privacy was traditionally associated with physical spaces and personal autonomy. However, the rise of digital technologies has transformed privacy into a complex, data-centric construct involving the collection, processing, and dissemination of

personal information (Solove, 2021). In the early internet era, privacy concerns centered on unauthorized access and data breaches. As online platforms matured, the focus shifted toward more nuanced threats such as behavioral tracking, algorithmic profiling, and the commodification of user data. Social media platforms have redefined the boundaries of privacy by encouraging voluntary disclosure while simultaneously enabling large-scale data harvesting (Nemec Zlatolas et al., 2022; Gruzd et al., 2020). The emergence of the "privacy paradox" where users express concern about privacy but continue to share personal information has further complicated the discourse (Gruzd & Hernández-García, 2022). Scholars have proposed models such as the Privacy Calculus to explain this behavior, suggesting that users weigh perceived benefits against potential risks when deciding what to disclose (Li & Lin, 2021). Contemporary discussions of data privacy now encompass not only individual rights but also collective harms, such as algorithmic discrimination and surveillance capitalism. These developments have prompted calls for stronger regulatory frameworks, ethical platform design, and user empowerment strategies (Martin, 2019; Shin, 2020).

2.2 Legal and Ethical Frameworks

Legal and ethical frameworks play a critical role in regulating how personal data is collected, processed, and protected on social media platforms. Globally, the General Data Protection Regulation (GDPR) has set a benchmark for user rights, transparency, and accountability in data handling. It mandates informed consent, data minimization, and breach notification, influencing privacy legislation worldwide (Reis et al., 2024). In Malaysia, the Personal Data Protection Act (PDPA) governs the use of personal data in commercial settings. While it outlines principles such as notice, choice, and security, enforcement remains inconsistent especially across e-commerce and social media platforms (Hamzah et al., 2018; Ali et al., 2025). Studies show that many platforms fail to comply fully with PDPA requirements, leaving users vulnerable to misuse and unauthorized sharing. Ethically, the rise of algorithmic decision-making and behavioral profiling has raised concerns about fairness, transparency, and user autonomy. Scholars argue that platforms must go beyond legal compliance to embrace ethical design principles that prioritize user dignity and informed control (Martin, 2019; Shin, 2020). The lack of clarity in privacy policies and the use of dark patterns further complicate ethical accountability. As digital ecosystems grow more complex, legal and ethical frameworks must evolve to address emerging threats such as AI-driven surveillance, cross-platform data aggregation, and consent fatigue. This section provides the foundation for evaluating platform compliance and user protection in later chapters.

2.3 Common Patterns of Data Misuse on Social Media

The misuse of personal data on social media platforms has become increasingly sophisticated, driven by commercial interests, algorithmic technologies, and weak regulatory enforcement. One of the most prevalent patterns is unauthorized data harvesting, where platforms collect far more information than users knowingly consent to. This includes metadata, behavioral signals, and third-party tracking that extends beyond the platform itself (Böyük, 2025; Zhang et al., 2022). Often, privacy policies are written in vague or overly technical language, making it difficult for users to understand the extent of data collection. Another concerning pattern is behavioral profiling, where algorithms analyze user interactions to infer preferences, vulnerabilities, and even political leanings. These insights are then used to manipulate user behavior through targeted advertising or content curation, raising ethical concerns about autonomy and informed consent (Martin, 2019; Boldyreva et al., 2018). The Cambridge Analytica scandal remains a prominent example of how personal data can be weaponized for political influence, exploiting psychological traits derived from social media activity.

Commercial exploitation of personal data is also widespread. Platforms monetize user information by selling access to advertisers and data brokers, often without explicit user approval. This commodification of identity transforms users into products, undermining the principles of data sovereignty and informed participation (Mouw et al., 2023; Gruzd et al., 2020). In many cases, users are unaware that their data is being repurposed for profit, especially when consent is buried in lengthy terms of service agreements. Finally, identity theft and data breaches remain persistent threats. Weak security protocols, poor compliance with data protection laws, and inadequate breach notification practices contribute to the exposure of sensitive personal information. High-profile incidents across platforms have revealed systemic vulnerabilities in how user data is stored and protected (Zhang et al., 2022; Prajapat et al., 2024). These breaches not only harm individuals but also erode public trust in digital platforms.

2.4 Impact on Users, Organizations, and Society

The misuse of personal data on social media platforms has far-reaching consequences that extend beyond individual users to affect organizations and society at large. For users, the most immediate impact is the erosion of privacy and autonomy. When personal information is collected, analyzed, and shared without informed consent, users lose control over their digital identities. This can lead to emotional distress, reputational harm, and in severe cases, identity theft or financial fraud (Zhang et al., 2022; Niu et al., 2025). The psychological toll is compounded by the "privacy paradox," where users feel conflicted between the desire for privacy and the convenience of digital services (Gruzd & Hernández-

García, 2022). For organizations, data misuse can result in significant reputational damage, legal penalties, and loss of consumer trust. Companies that fail to comply with data protection laws such as the GDPR or Malaysia's PDPA may face fines, litigation, and public backlash (Ali et al., 2025; Reis et al., 2024). Beyond regulatory consequences, data breaches can disrupt operations, expose trade secrets, and weaken stakeholder confidence. Ethical lapses in data handling such as manipulative algorithms or opaque privacy policies can also undermine brand credibility and employee morale (Martin, 2019; Shin, 2020). At the societal level, unchecked data exploitation contributes to broader issues such as surveillance capitalism, algorithmic bias, and democratic erosion. When platforms use personal data to manipulate public opinion or suppress dissent, the integrity of civic discourse is compromised (Boldyreva et al., 2018; Fernando et al., 2025). Moreover, the normalization of data commodification reinforces structural inequalities, as marginalized groups are often disproportionately targeted or excluded by algorithmic systems. The societal cost is a digital environment where trust, fairness, and accountability are increasingly difficult to sustain.

3. Methodology

This study adopts a qualitative research approach, combining case analysis, literature synthesis, and conceptual modeling to investigate the misuse of personal data on social media platforms. The methodology is designed to capture both practical incidents and theoretical insights, enabling a comprehensive understanding of privacy risks and mitigation strategies.

3.1 Analysis of Real-World Attack Vectors

A significant portion of this study is dedicated to examining real-world case studies where social engineering techniques were successfully deployed. Case-based analysis allows for a grounded understanding of how different tactics are used, how victims respond, and what psychological levers are manipulated.

Cases	Description
The 2018 Cambridge Analytica Data Harvesting Scandal	In 2018, Cambridge Analytica was exposed for harvesting personal data from over 87 million Facebook users without their explicit consent. The firm used a personality quiz app that collected not only data from users who installed it, but also from their entire friend networks This data was then used to build psychological profiles and deliver targeted political ads during the U.S. presidential election and Brexit campaign. The scandal revealed how seemingly benign apps could be weaponized for mass data extraction and manipulation. It also highlighted Facebook's failure to enforce data usage policies and notify users promptly. The incident triggered global regulatory scrutiny and led to Facebook being fined $5 billion by the U.S. Federal Trade Commission (Boldyreva et al., 2018).
The 2022 iPay88 Payment Gateway Breach in Malaysia	In August 2022, Malaysian payment gateway provider iPay88 confirmed a cybersecurity breach that compromised cardholder data processed through its system. The breach affected multiple e-commerce platforms and raised concerns about the security of online transactions in Malaysia. Although the company claimed that no fraudulent transactions were detected, the incident triggered investigations by Bank Negara Malaysia and public calls for stricter enforcement of the Personal Data Protection Act (PDPA). The breach exposed weaknesses in third-party payment integrations and highlighted the need for stronger encryption, breach notification protocols, and vendor accountability (Ali et al., 2025; Exabytes, 2023)
The 2023 Telekom Malaysia Data Leak Allegation	In January 2024, a hacker asserted the theft of Telekom Malaysia's customer database, which included roughly 20 million user records.The alleged breach included sensitive information such as names, contact details, and service usage data. Telekom Malaysia responded by launching an internal investigation and engaging authorities, stating that the leaked data appeared to be "pre-processed and recycled." Despite this, the incident sparked public concern over data governance in Malaysia's telecom sector and emphasized the importance of proactive breach detection, transparency, and regulatory oversight

Table 2 : Real-World Attack Vectors

3.2 Review of Empirical Studies and Cybersecurity Reports

This study conducted a targeted review of empirical research and privacy breach reports published between 2018 and 2025. The review focused on studies that examined user behavior, platform compliance, and the effectiveness of privacy safeguards in social media and e-commerce contexts. Empirical findings from Gruzd and Hernández-García (2022) revealed how users navigate the privacy paradox, often employing risk mitigation strategies such as selective disclosure and identity masking. These behavioral insights were critical in understanding how users respond to perceived threats despite limited control over platform settings. Several studies also evaluated the effectiveness of privacy policies and regulatory enforcement. Böyük (2025) analyzed the privacy policies of major social media platforms and found widespread use of vague language and inconsistent data handling practices. Similarly, Ali et al. (2025) assessed Malaysian e-commerce platforms and discovered frequent non-compliance with the Personal Data Protection Act (PDPA), especially in areas related to consent and breach notification. These findings were supported by breach reports such as the 2022 iPay88 incident, which exposed weaknesses in third-party payment integrations and triggered regulatory scrutiny from Bank Negara Malaysia. Technical analyses from Zhang et al. (2022) and Prajapat et al. (2024) provided insights into the nature of data breaches, including common attack vectors, encryption failures, and post-breach response gaps. These studies emphasized the need for robust cybersecurity infrastructure and proactive monitoring to prevent unauthorized access. Additionally, Reis et al. (2024) offered a global perspective on privacy law enforcement, highlighting disparities in regulatory capacity and the challenges of cross-border data governance.

Together, these empirical sources enriched the study's understanding of privacy risks by offering both user-centric and system-level perspectives. They also informed the development of the evaluation framework presented in the next section, which integrates behavioral models and technical standards to assess privacy vulnerabilities.

3.3 Framework for Evaluating Human Vulnerability

To systematically assess privacy risks on social media platforms, this study adopts a hybrid evaluation framework that integrates both behavioral and technical perspectives. The first component is the Privacy Calculus model, which explains how users make decisions about personal data disclosure. According to this model, individuals weigh perceived benefits such as convenience, personalization, and social connectivity against potential risks like data misuse, surveillance, and identity theft (Li & Lin, 2021). This framework is particularly relevant in understanding the privacy paradox, where users continue to share sensitive information despite expressing concern over their digital privacy (Gruzd & Hernández-García, 2022).

Figure 1 : CIA Triad. negg.blog Group (2024)

The second component is the CIA Triad, a fundamental concept in cybersecurity that assesses systems according to three principles: Confidentiality, Integrity, and Availability. Confidentiality pertains to safeguarding personal data from unauthorised access; Integrity maintains the accuracy and unaltered state of data; and Availability assures that data and services are accessible as required. The study evaluates platform vulnerabilities, breach response mechanisms, and adherence to data protection standards through the use of the CIA Triad (Shin, 2020; Zhang et al., 2022). Together, these frameworks provide a multidimensional lens for evaluating privacy risks. The Privacy Calculus captures user behavior and decision-making, while the CIA Triad addresses infrastructural and regulatory safeguards. This dual approach enables a comprehensive analysis of how privacy violations occur, how they affect stakeholders, and what measures can be taken to mitigate them.

4. Current Preventive Measures

As privacy risks on social media platforms continue to escalate, various preventive measures have been introduced to protect users and promote responsible data governance. These measures span technical controls, legal enforcement, and educational initiatives, each addressing different aspects of the privacy ecosystem.

4.1 Privacy Settings and User Controls

Most social media platforms now offer customizable privacy settings that allow users to manage who can view their content, access their personal information, and interact with their profiles. Features such as two-factor authentication, ad preference controls, and data download options empower users to exercise greater control over their digital footprint. However, studies show that many users either overlook these settings or find them difficult to navigate due to poor interface design and lack of clarity (Böyük, 2025; Shin, 2020). Moreover, default settings often favor data sharing, requiring users to opt out manually. While these controls are essential, their effectiveness depends heavily on user awareness and platform transparency.

4.2 Regulatory Enforcement and Platform Compliance

Legal frameworks such as the General Data Protection Regulation (GDPR) and Malaysia's Personal Data Protection Act (PDPA) provide formal mechanisms for protecting user data. These laws mandate informed consent, breach notification, and data minimization practices. Regulatory bodies have also begun issuing fines and compliance orders to platforms that violate privacy standards, as seen in the Facebook-Cambridge Analytica case and the iPay88 breach investigation (Ali et al., 2025; Boldyreva et al., 2018). Despite these efforts, enforcement remains uneven, especially in regions with limited regulatory capacity or outdated legislation. Many platforms operate across borders, complicating jurisdictional oversight and slowing down response times. Strengthening enforcement mechanisms and updating legal definitions of consent and profiling are critical to improving compliance.

4.3 Awareness Campaigns and Digital Literacy

Educational initiatives aimed at improving digital literacy have emerged as a key strategy in empowering users to protect their privacy. Campaigns led by governments, NGOs, and academic institutions focus on teaching users how to identify phishing attempts, configure privacy settings, and understand terms of service. In Malaysia, efforts to integrate cybersecurity awareness into school curricula and public service announcements have shown promise, though coverage remains limited (Hamzah et al., 2018; Fernando et al., 2025). Digital literacy is especially important in combating consent fatigue and dark patterns, as informed users are more likely to question manipulative design and demand accountability. However, these campaigns must be sustained, inclusive, and adapted to evolving threats to remain effective.

5. Future Threats and Emerging Trends

As digital ecosystems continue to evolve, new challenges are emerging that complicate efforts to safeguard personal data. These trends reflect both technological advancements and regulatory gaps, requiring proactive strategies from users, developers, and policymakers.

5.1 AI-Driven Profiling and Behavioral Targeting

Artificial intelligence has markedly improved the accuracy and extent of behavioural profiling. Social media platforms utilise machine learning algorithms to analyse user behaviour, predict preferences, and provide hyper-targeted content. The growth of personalisation also introduces ethical issues related to manipulation, discrimination, and the erosion of autonomy. AI-driven profiling has the capacity to deduce sensitive characteristics, including political beliefs, mental health conditions, and intent to buy, frequently without the explicit consent of users (Tufekci, 2021; Zhang et al., 2022). The lack of transparency in algorithmic decision-making hinders users' comprehension of data usage, while existing privacy settings provide insufficient control over these mechanisms. The advancement of AI increases the potential for exploitative targeting and surveillance, necessitating enhanced transparency and accountability in algorithms.

5.2 Cross-Platform Data Tracking and Surveillance

Another emerging threat is the integration of user data across multiple platforms and services. Companies that own several digital products such as Meta's Facebook, Instagram, and WhatsApp can aggregate user data to build unified profiles that span different contexts. This cross-platform tracking enables deeper behavioral insights but also increases surveillance risks and reduces user visibility into how their data is linked and reused. The lack of interoperability standards and opt-out mechanisms makes it difficult for users to manage their privacy across ecosystems. Moreover, data sharing agreements between platforms and third-party advertisers often operate in legally gray areas, further complicating enforcement and user protection (Fernando et al., 2025; Shin, 2020).

5.3 Gaps in Policy and Enforcement Mechanisms

Despite the existence of privacy laws such as the GDPR and PDPA, enforcement remains inconsistent and reactive. Many regulations struggle to keep pace with technological innovation, leaving loopholes in areas like AI profiling, biometric data, and cross-border data flows. In Malaysia, for example, the PDPA does not apply to government agencies and lacks provisions for algorithmic transparency or platform interoperability (Ali et al., 2025). Regulatory bodies often lack the resources or jurisdictional reach to investigate violations effectively, especially when platforms operate globally. These gaps undermine user trust and limit the effectiveness of legal safeguards. Future policy

development must address emerging threats, strengthen enforcement capacity, and promote international cooperation to ensure comprehensive data protection.

6. Conclusion

This study has explored the multifaceted issue of personal data misuse on social media platforms, drawing from real-world cases, empirical research, and conceptual frameworks. The analysis revealed recurring patterns of unauthorized data harvesting, behavioral profiling, commercial exploitation, and weak breach response each contributing to a growing erosion of user trust and digital autonomy. Through the integration of the Privacy Calculus and CIA Triad, the study provided a dual lens for evaluating privacy risks from both behavioral and technical perspectives. Preventive measures such as privacy settings, regulatory enforcement, and digital literacy campaigns offer partial protection, but they remain limited by user awareness, platform design, and enforcement capacity. Emerging threats including AI-driven profiling, cross-platform surveillance, and policy gaps highlight the urgent need for more adaptive, transparent, and inclusive privacy governance. Ultimately, safeguarding personal data in the age of social media requires a collaborative effort among users, developers, regulators, and educators. Platforms must prioritize ethical design and transparency, while policymakers must strengthen legal frameworks to address evolving risks. Users, in turn, must be empowered through education and intuitive controls to make informed decisions about their digital identities. This study contributes to that effort by mapping the landscape of data misuse and offering a foundation for future research, policy development, and platform accountability.

Acknowledgments

The authors would like to thank all members of the School of Computing who are involved in this study. This work was supported by Universiti Utara Malaysia.

References

AlMudahi, G. F., AlSwayeh, L. K., AlAnsary, S. A., & Latif, R. (2022). Social media privacy issues, threats, and risks. *2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU)*, 155–159. https://doi.org/10.1109/wids-psu54548.2022.00043

Boldyreva*, E. L., Grishina, N. Y., & Duisembina, Y. (2018). Cambridge analytica: ethics and online manipulation with decision-making process. *The European Proceedings of Social and Behavioural Sciences*, 91–102. https://doi.org/10.15405/epsbs.2018.12.02.10

Böyük, M. (2025). User data and digital privacy: privacy policies of social media platforms. *Turkish Online Journal of Design Art and Communication*, *15*(1), 225–239. https://doi.org/10.7456/tojdac.1569287

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Fernando, Z. J., Widyawati, A., & Rinaldi, K. (2025). Cyber victimology and legal gaps in southeast asia. *International Law Discourse in Southeast Asia*, *4*(1), 1–39. https://doi.org/10.15294/ildisea.v4i1.20147

G, R., K M, K. R., Ankolekar, A., Kamath, G. P., & Naik, V. V. (2025). Data privacy and ethics on social media platforms. *2025 3rd International Conference on Inventive Computing and Informatics (ICICI)*, 410–415. https://doi.org/10.1109/icici65870.2025.11069689

Gruzd, A., & Hernández-García, Á. (2022). A balancing act: How risk mitigation strategies employed by users explain the privacy paradox on social media. *Behaviour & Information Technology*, *43*(1), 21–39. https://doi.org/10.1080/0144929x.2022.2152366

Gruzd, A., Jacobson, J., & Dubois, E. (2020). Cybervetting and the public life of social media data. *Social Media + Society*, *6*(2). https://doi.org/10.1177/2056305120915618

Hamzah, M. A., Ahmad, A. R., Hussin, N., & Ibrahim, Z. (2019). Personal data privacy protection: A review on malaysia's cyber security policies. *International Journal of Academic Research in Business and Social Sciences*, *8*(12). https://doi.org/10.6007/ijarbss/v8-i12/5251

Hui, X. (2023, April 17). *Exabytes network sdn. bhd.* Exabytes Blog. https://www.exabytes.my/blog/data-breaches-exposed-malaysia/

Ifinedo, P., Vachon, F., & Ayanso, A. (2024). Reducing data privacy breaches: An empirical study of relevant antecedents and an outcome. *Information Technology & People*, *38*(4), 1712–1734. https://doi.org/10.1108/itp-07-2022-0516

Jian, N. J., & Kamsin, I. F. B. (2021). Cybersecurity awareness among the youngs in Malaysia by gamification. *Atlantis Highlights in Computer Sciences*. https://doi.org/10.2991/ahis.k.210913.061

Martin, K. (2018). Ethical implications and accountability of algorithms. *Journal of Business Ethics*, *160*(4), 835–850. https://doi.org/10.1007/s10551-018-3921-3

Mouw, S., Tutuarima, F., & Hatala, R. (2023). Misuse of personal data for commercial purposes on facebook social media as a digital crime and legal certainty for users. *JETISH: Journal of Education Technology Information Social Sciences and Health*, *2*(2), 1196–1203. https://doi.org/10.57235/jetish.v2i2.590

Nemec Zlatolas, L., Hrgarek, L., Welzer, T., & Hölbl, M. (2022). Models of privacy and disclosure on social networking sites: a systematic literature review. *Mathematics*, *10*(1), 146. https://doi.org/10.3390/math10010146

Niu, J., Mazhar, B., Ul Haq, I., & Maqsood, F. (2025). Protecting privacy on social media: Mitigating interpersonal conflicts through identity masking and suspended use, with a mediating role of privacy concerns and online information disclosure awareness. *Current Psychology*, *44*(4), 2722–2734. https://doi.org/10.1007/s12144-025-07364-3

Oluwatosin Reis, Nkechi Emmanuella Eneh, Benedicta Ehimuan, Anthony Anyanwu, Temidayo Olorunsogo, & Temitayo Oluwaseun Abrahams. (2024). Privacy law challenges in the digital age: a global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences*, *6*(1), 73–88. https://doi.org/10.51594/ijarss.v6i1.733

Prajapat, S., Gaur, A. S., Soni, P., Nagar, N., & Goswami, P. (2024). Cyber attacks and review of recent data breach incidents their trends and measures. In *Lecture Notes in Networks and Systems* (pp. 549–576). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74443-3_33

Purificato, Erasmo. (2024, February). *User modeling and user profiling: A comprehensive survey*. https://arxiv.org/html/2402.09660v2

Shehu Ali, A., Zaaba, Z. F., Mahinderjit Singh, M., Anuar, N. B., & M. Shariff, M. R. (2025). Creating and analysing privacy policies of Malaysia e-commerce using personal data protection act. *Bulletin of Electrical Engineering and Informatics*, *14*(3), 2404–2412. https://doi.org/10.11591/eei.v14i3.8991

Shin, D. (2020). User perceptions of algorithmic decisions in the personalized AI system: perceptual evaluation of fairness, accountability, transparency, and explainability. *Journal of Broadcasting & Electronic Media*, *64*(4), 541–565. https://doi.org/10.1080/08838151.2020.1843357

Solove, D. J. (2021). *A taxonomy of privacy*.

Yeoh, A. (2024, January 26). Hacker alleges to have stolen Telekom Malaysia's customer database with 'nearly 20 million effective user data' (Updated with TM's statement). *The Star*. https://www.thestar.com.my/tech/tech-news/2024/01/26/hacker-alleges-to-have-stolen-telekom-malaysias-customer-database-with-nearly-20-million-effective-user-data

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D. P., & Ghorbani, A. A. (2022). Data breach: Analysis, countermeasures and challenges. *International Journal of Information and Computer Security*, *19*(3/4), 402. https://doi.org/10.1504/ijics.2022.127169