Revisiting the Privacy Paradox through Facebook Pro: User Behavior and Collaborative Policy Design

Nadya Mentari[1][0009-0001-9724-9106]1, Baiq Syofiatun Yuhaniza[2], Putri Fajar Ayu Hendrayani[3][0009-0005-8844-5462]3

[1 2 3] Master of Library and Information Science, Universitas Indonesia, Depok, Indonesia
nadyamentari.nm@gmail.com[1], syofiatun.yuhaniza07@gmail.com[2], putrifay30@gmail.com[3]

Abstract. This study examines how Facebook Pro users perceive and manage privacy in their everyday digital practices, with particular attention to the relationship between privacy awareness and information-sharing behavior. Using a qualitative case study approach, the research focuses on five purposively selected users who actively share content and engage with Facebook Pro's extended features. Data were collected during March–April 2024 through written interviews, observation of users' public posts, and analysis of relevant legal frameworks, particularly Indonesia's Personal Data Protection Law (Law No. 27/2022). Thematic analysis revealed that although users expressed awareness of privacy risks, they often shared identifiable content without activating privacy controls. This behavioral gap aligns with the concept of the privacy paradox, wherein users' stated concerns do not translate into protective actions. In addition, participants demonstrated limited understanding of platform settings and the legal rights available to them under the PDP Law. While the study is limited by its small sample size and context-specific scope, the findings offer important implications for policy and platform governance. The results suggest that digital privacy cannot be addressed solely at the individual level; rather, it requires collaborative efforts involving users, service providers, and regulators. The study contributes to ongoing discussions on digital privacy by situating user behavior within a broader sociotechnical and regulatory landscape.

Keywords: Privacy Paradox, Facebook Pro, Information Behavior, Platform Governance

1 Introduction

The rapid advancement of digital technologies has profoundly reshaped how individuals and professionals engage in information exchange, with social media serving as a key space for personal expression, professional branding, and civic participation. Facebook Pro, an enhanced variant of the platform, offers broader reach and engagement but also raises higher risks for privacy management. The persistence of the privacy paradox—users' concern for privacy contrasting with their willingness to disclose personal content—illustrates the tension between individual behavior, platform design, and social norms.

In Indonesia, growing cases of impersonation, phishing, and identity theft make digital privacy a pressing issue. Although the Personal Data Protection Law (Law No. 27/2022) establishes a legal foundation, its effectiveness is limited by weak awareness and uneven enforcement. This study examines how Facebook Pro users manage privacy and highlights the need for collaborative governance, where users, platforms, and regulators share responsibility in balancing openness with protection.

2 Literature Review

2.1 Information Policy and Platform Governance

IInformation policy encompasses the principles and mechanisms that regulate how data is created, accessed, and controlled (Braman, 2006). In platform ecosystems, governance extends beyond state regulation to include private rules terms of service, algorithmic curation, and privacy settings (Gorwa, 2019). For Facebook Pro, this layered governance environment directly shapes the user's perception of privacy options.

2.2 Information Disclosure and Privacy Decision-Making

The privacy calculus model suggests users weigh perceived benefits of disclosure against potential risks (Culnan & Armstrong, 1999). Yet users often underestimate risks or lack understanding of settings, leading to over-disclosure. The paradox emerges as individuals express high concern but still disclose, due in part to bounded rationality (Simon, 1955), limited time, knowledge, and cognitive resources.

2.3 Indonesian Regulatory Context

The PDP Law (2022) codifies individual rights over personal data and places obligations on data controllers. However, widespread lack of legal literacy limits its impact. The study situates user behavior against this regulatory context, highlighting the tension between formal protection and lived digital practice.

3 Methodology

This study used a qualitative case study approach to explore how Facebook Pro users perceive and manage privacy in everyday digital practices. Conducted between March and April 2024, the research involved five purposively selected users with at least 1,000 followers, frequent use of hashtags such as #FbPro and #jangkauanluas, and active content sharing. Pseudonyms were assigned to protect participant identities.

Data were collected using three qualitative techniques: (1) written interviews, (2) observation of content shared by informants on their Facebook Pro profiles, and (3) analysis of relevant legal documents, particularly the Indonesian Personal Data Protection Law (Law No. 27/2022). The data were analyzed descriptively, focusing on

emerging themes and patterns, particularly the gaps between stated privacy awareness and actual behavior. Triangulating these data sources enabled a deeper understanding of how users navigate privacy within the broader sociotechnical system of Facebook Pro.

4 Findings

4.1. Informant Profile

This study involved five purposively selected Facebook Pro users (four women and one man), aged 25–34, all familiar with the platform's features and active in daily or near-daily use. While three had higher education and two had secondary education, backgrounds influenced how they articulated motivations and privacy perspectives. Their purposes varied, ranging from business promotion and content creation to social interaction and self-expression. These profiles, though not representative of broader populations, provide contextual insights into how users experience and respond to privacy concerns within Facebook Pro.

4.2. User Intentions and Content Sharing Practices on Facebook Pro

The five informants described varied motivations for using Facebook Pro, ranging from income generation through online selling and content monetization to amusement, distraction, and social networking. Some used the platform to promote products or expand their networks, while others relied on it for lifestyle expression. Most readily shared photos and videos of daily routines, cooking, or promotional activities, and a few disclosed personal details such as marital status, education, or occupation. While they avoided highly sensitive information like health or financial data, their content still revealed identifiable traces, underscoring the platform's dual role as both personal and semi-professional space.

Attitudes toward privacy varied. Although some informants expressed concern about fraud, impersonation, or identity theft, others disclosed content with little hesitation. Awareness of risks did not always lead to protective actions, reflecting the privacy paradox. Informants often relied on habits or convenience rather than deliberate choices, consistent with bounded rationality. Few were familiar with Facebook Pro's privacy features, and most were unaware of rights under Indonesia's Personal Data Protection Law (No. 27/2022). This gap in digital and legal literacy highlights the need for not only user education but also stronger communication and accountability from platforms and regulators.

4.3. Observed Patterns of Digital Disclosure

Observation revealed diverse disclosure practices among Facebook Pro users, ranging from seemingly harmless lifestyle content to highly sensitive documents. For example as can be seen in Figure 1, a simple video of cooking a chicken steak, while benign in appearance, exposed behavioral routines, locations, and time-specific details that could

accumulate into identifiable digital traces. Such everyday posts illustrate how ordinary sharing can create long-term privacy risks often unnoticed by users.

Fig. 1. Example of Content Shared by Informant on Facebook pro

Another observed post on Figure 2 contained economic disclosures also carried risks. One user posted a price list for bouquets and snacks to promote a home business, reflecting the informal nature of economic activity on social media. While serving a business purpose, such posts lacked privacy safeguards and, when combined with other identifiable data, heightened vulnerability to unsolicited contact or financial exploitation. This underscores how self-presentation online often occurs outside of formal policy protections.

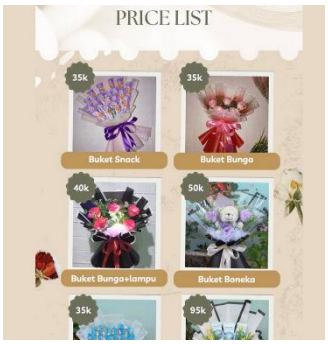

Fig. 2. Example of Content Shared by Informant on Facebook pro

The most concerning in Figure 3 case' was a public post of a Marriage Agreement Letter containing full legal names, birth dates, and signatures. This stark example of the privacy paradox highlights how users, constrained by bounded rationality, may knowingly expose private information without anticipating long-term consequences. These patterns point to broader gaps in platform responsibility and regulatory enforcement. Without automated warnings, intuitive controls, or strong legal communication, users remain at risk. Effective solutions therefore require combining

user education with structural interventions, ensuring privacy is embedded in both platform design and enforceable data protection policies.

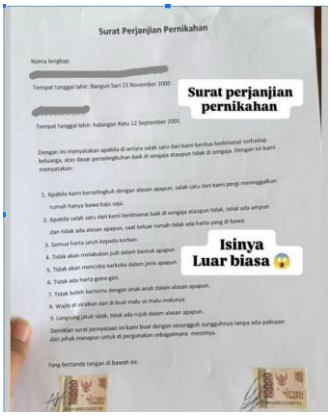

Fig. 3. Example of Content Shared by Informant on Facebook pro

4.4. Collaborative Policy Design

The findings highlight that Facebook Pro users, though generally educated and digitally literate, often display contradictions between their awareness of privacy risks and their protective actions. This gap reflects not negligence but structural challenges shaped by platform governance, where responsibility is distributed among governments, platforms, and civil society. Addressing this requires collaborative governance (Ansell & Gash, 2008), with users as active participants in shaping data management, and the adoption of Privacy by Design (Cavoukian, 2009), which embeds privacy into system architecture through proactive policies, default protections, and intuitive design. Platforms must strengthen accountability with real-time alerts, simplified controls, and transparent consent, while regulators must ensure laws like Indonesia's PDP Law are effectively enforced. Ultimately, safeguarding digital privacy is a shared responsibility requiring inclusive governance, institutional support, and enforceable protections to close the gap between user concerns and actual practices.

5 Conclusion

This study examined how Facebook Pro users perceive and manage privacy, showing that while they express awareness of risks, they continue sharing personal routines, business details, and even sensitive documents without sufficient safeguards, reflecting the persistence of the privacy paradox. Limited knowledge of platform settings and Indonesia's PDP Law further weakens protection, highlighting that privacy cannot rest solely on individuals but requires collaborative governance among users, platforms, and regulators. Although limited by a small, context-specific sample, the findings emphasize the need for stronger platform accountability, effective policy enforcement,

and user engagement, with future research exploring broader populations and the impact of interventions such as privacy prompts and simplified policy tools.

References

1. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. *Science* 347(6221), 509–514 (2015).
2. Ansell, C., Gash, A.: Collaborative governance in theory and practice. *J. Public Adm. Res. Theory* 18(4), 543–571 (2008).
3. Boyd, D.M., Ellison, N.B.: Social network sites: Definition, history, and scholarship. *J. Comput.-Mediat. Commun.* **13**(1), 210–230 (2007).
4. Braman, S.: Change of State: Information, Policy, and Power. MIT Press, Cambridge (2006)
5. Cavoukian, A.: Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada (2009).
6. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. *Information Systems Research* **17**(1), 61–80 (2006)
7. Creswell, J.W., Creswell, J.D.: Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 5th edn. SAGE Publications, Thousand Oaks (2018)
8. Debatin, B., Lovejoy, J.P., Horn, A.K., Hughes, B.N.: Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *J. Comput.-Mediat. Commun.* **15**(1), 83–108 (2009)
9. Duff, A.S.: The past, present, and future of information policy: Towards a normative theory of information policy. *Inf. Res.* **9**(1) (2004)
10. Gorwa, R.: What is platform governance? *Inf. Commun. Soc.* **22**(6), 854–871 (2019).
11. Gorwa, R.: The platform governance triangle: Conceptualizing the informal regulation of online content. *Internet Policy Rev.* **8**(2) (2019). https://policyreview.info/articles/analysis/platform-governance-triangle
12. Nabila, S., Dewi, M.S.W., Hilaly, S.G., Mukaromah, S.: Analisis tingkat kesadaran pengguna media sosial terkait privasi dan keamanan data pribadi. In: *Proc. Sem. Nas. Teknologi dan Sistem Informasi (SITASI) 2023*, pp. 553–560. UPN Veteran Jawa Timur (2023)
13. Pemerintah Republik Indonesia: Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (2022)
14. Revilia, D., Irwansyah: Literasi media sosial: Kesadaran keamanan dan privasi dalam perspektif generasi milenial. *J. Penelit. Komun. dan Opini Publik* **24**(1), 1–15 (2020).
15. Simon, H.A.: A behavioral model of rational choice. Q. J. Econ. 69(1), 99–118 (1955)
16. van de Worp, S.: The ability of users of social networking sites to accurately perform the privacy calculus: An empirical study on the disclosure abilities of Facebook users. Master's thesis, University of Twente (2014)