Jurnal Komunikasi
Vol. 3 No. 1 2025, hal. 154-160 e-ISSN: 2988-1331

POTENTIAL FOR PRIVACY VIOLATIONS BY MOBILE APPLICATIONS: A LITERATURE REVIEW OF LEGAL STUDIES

Loso Judijanto
IPOSS Jakarta, Indonesia
losojudijantobumn@gmail.com

Abstract

Mobile applications, with their ability to collect and process user data, raise significant privacy concerns. This literature study critically evaluates the risks of possible privacy violations and how applicable legal regulations address these issues. It was found that many applications fail to obtain clear consent from users and are often not transparent in their data collection and processing practices. In addition, sharing data with third parties without adequate safeguards increases the risk of data leakage. Through a legal perspective, this study emphasises the importance of transparency, data protection, and accountability of application developers in maintaining user privacy. This study underlines that a comprehensive approach to regulation and the strict application of privacy principles are essential to reduce the risk of violations and protect user rights.
Keywords: Potential, Violation, Privacy, Mobile Applications, Legal Review literature.

Introduction

Since the current rapid development of the digital era, mobile applications have become an integral part of everyday life. Mobile applications are used for various purposes, ranging from communication, entertainment, education, to financial services. Their existence provides convenience and comfort for users.

Mobile applications are software designed to run on mobile devices, such as smartphones and tablets. These applications are usually developed for specific operating systems, such as Android or iOS, and distributed through application distribution platforms such as the Google Play Store or the Apple App Store. Mobile applications can be divided into several categories based on their functions, such as productivity applications, games, social media, financial management, education, and many more. They offer intuitive user interfaces and are designed to utilise the capabilities of mobile devices, such as cameras, GPS, and motion sensors (Zang et al., 2020).

The main purpose of mobile applications is to provide convenience and increase efficiency in various aspects of users' lives. For example, banking applications make it easy for users to conduct financial transactions, monitor account balances, and manage investments directly from their mobile phones. Social media applications allow users to connect and interact with friends and family without geographical boundaries (Reed & Foster, 2023). Educational applications provide access to various learning and training materials that can be accessed anytime and anywhere. Overall, mobile applications are

designed to enhance the user experience by providing quick and easily accessible solutions for various daily needs (Wang & Chen, 2023).

According to the latest data, the number of smartphone users in Indonesia has reached more than 160 million people, most of whom actively use various mobile applications. However, behind all the benefits offered by mobile applications, there is a potential risk to user privacy. Many mobile applications collect, store, and process users' personal data without adequate knowledge or consent. The data collected can include personal information such as name, address, telephone number, contacts, location, and user habits and preferences. This non-transparent data collection opens up opportunities for privacy violations (Schmidt & Hurst, 2020).

Privacy violations can have far-reaching and serious impacts on individuals and organisations. For individuals, the most immediate impact is the risk of identity theft, where personal information that falls into the wrong hands can be used for fraud or other criminal acts. This can result in considerable financial loss, reputational damage, and emotional distress (Gomez & Linares, 2025). In addition, breaches of privacy can also reduce individuals' trust in digital systems and online services, reducing the use of technology and participation in digital platforms. For organisations, the impact of privacy breaches includes significant regulatory fines, lawsuits, reputational damage, and loss of customer trust, all of which can affect overall business performance. Negligence in protecting user data can also have legal implications and strict supervision from regulatory authorities (Wang & Chen, 2023).

A number of privacy violations have come to light, such as the Cambridge Analytica case, which successfully accessed the personal data of millions of Facebook users without permission. This case highlights how fragile privacy protection is in the digital age and raises concerns about similar actions by other mobile applications. Protecting user privacy is a complex challenge because it involves not only technical aspects, but also legal aspects (Garcia, 2022). A review of the existing legal framework shows that privacy regulations in Indonesia still have many weaknesses and shortcomings in anticipating various forms of privacy violations by mobile applications. For example, the Electronic Information and Transactions Law (ITE Law) and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions have not fully regulated in detail the protection of personal data of mobile application users (Lee & Park, 2019).

Therefore, it is important to understand more about the potential for privacy violations by mobile applications and how the existing legal framework can protect user privacy. This study focuses on a legal review literature study to analyse and find answers to this problem. Through this study, it is hoped that useful recommendations can be generated for policy makers, application developers, and users to improve privacy protection in the digital age.

Research Methods

The study in this research uses the literature method. The literature research method is an approach used to collect, analyse, and evaluate various published sources of information related to a specific research topic. This process involves searching and reading scientific journals, books, research reports, theses, dissertations, articles, and other secondary sources to gain an in-depth and comprehensive understanding of the field of study under investigation (Rofiah & Bungin, 2021); (Yusanto, 2020). Literature research aims to identify trends, discover various existing perspectives, reveal research gaps, and support arguments with previously tested evidence. By synthesising existing information, researchers can build a strong theoretical foundation, formulate hypotheses, and develop methodologies for further research. This method is essential in ensuring that the research conducted has a strong foundation and is relevant to the broader academic or practical context (Sudrajat & Moha, 2019).

Results and Discussion

Potential Privacy Violations by Mobile Applications

Privacy violations by mobile applications are currently a serious concern for users all over the world. With the large number of applications available on platforms such as iOS and Android, users‘ personal data has the potential to be misused by irresponsible application developers. Mobile applications can access various types of users’ personal data, ranging from location, contact, photo, to browsing history. Often, this data access permission is given by users without fully understanding the risks involved, opening up opportunities for privacy violations (Hernandez & Ortega, 2022).

One potential privacy violation is the unlawful collection of location data. Although it is used to provide better services, such as recommendations for nearby restaurants or directions, this location data can also be used by third parties to monitor users' habits and movements. This information can be sold to advertisers or even criminals with malicious intent. Crimes such as stalking or theft planned based on user location data are a very real threat (Feng & Xie, 2021).

In addition, mobile applications can also access contacts and other personal information without the user's knowledge. Contact data can be used to send spam or advertising messages automatically without the device owner's permission. Often, applications request access to user contacts when they are first downloaded on the grounds of improving service or user experience. However, without adequate protection, this information can be easily exploited for commercial or criminal purposes (Olsen & Meyers, 2021).

Mobile applications that request access to photo galleries and cameras have the potential to violate user privacy in a more personal way. Personal photos, videos, and even audio recordings can be accessed and used without explicit consent. Extreme cases can involve active recording from cameras or microphones without the user's

knowledge, which is a major violation of individual privacy and security rights (Johnson & Stewart, 2020).

In addition, there are privacy issues related to the monetisation of user data. Many mobile applications operate on a business model that involves selling user data to third parties, including advertising and market research companies. Without strict regulation, the scale and use of the data collected is often not transparent to users. This not only raises ethical concerns but also puts users at risk of data breaches (Henderson & Booth, 2022).

Further risks come from the security of the application itself. Many applications, especially those developed by little-known or untrusted third parties, may not have adequate security mechanisms to protect user data. The vulnerability to hacking, malware, and cyberattacks is very high, which can lead to sensitive data falling into the hands of hackers. Users can become victims of identity theft, bank account drain, or phishing attacks designed to steal further information (Fischer & Keller, 2021).

Therefore, to mitigate the risk of privacy violations by mobile applications, it is important for users to be more selective and vigilant in granting data access permissions. Reading the privacy policy, evaluating the permissions requested by the application, and choosing applications from trusted sources are important steps. At the regulatory level, governments and regulatory bodies need to tighten controls on how user data is collected and used by mobile applications, to ensure that user privacy and security remain a priority.

Legal Review Regarding Privacy Violations on Mobile Applications

Legal reviews regarding privacy violations on mobile applications are becoming increasingly relevant with the advancement of technology and the rampant use of mobile devices. In a legal context, the privacy of mobile application users is protected by various regulations at both the national and international levels. These privacy concerns include the collection, use, and dissemination of users' personal data without their knowledge or consent. The regulations that are implemented aim to provide more protection to users and ensure that technology companies comply with established privacy standards (Silva & Branco, 2023).

In Indonesia, rules related to digital privacy are mainly regulated by the Electronic Information and Transactions Law (UU ITE) and the recently passed Personal Data Protection Law (UU PDP). These laws mandate that personal data must be collected with the consent of the data owner and may only be used for specific, clear purposes. Violation of this provision can result in administrative to criminal sanctions for the perpetrator, especially for companies that fail to maintain the confidentiality of their consumer data (Li & Wong, 2022).

At the international level, there is the General Data Protection Regulation (GDPR) which is applied in the European Union and affects global companies that have

a user base in the region. The GDPR is considered the gold standard in personal data protection, emphasising the rights of data subjects and imposing heavy fines on violators. This rule forces mobile application companies to implement stricter protection mechanisms, including more transparent notifications and easier data deletion mechanisms for users (Kim, 2024).

Privacy issues also include mobile applications that access data that is not necessary for their functionality, such as accessing a user's contacts or location for no apparent reason. This poses a risk of personal data leaks that can be misused by third parties. Legal provisions require that every data access request must be made with clear notification and explicit consent from the user, and failure to do so can be considered a violation of the law (Vani et al., 2023).

The main challenge in enforcing the law regarding mobile app privacy is the borderless nature of the internet, where apps can be developed in one country and operated in another. This complexity often complicates law enforcement and encourages international cooperation between relevant authorities. For example, many countries are now cooperating in terms of exchanging information and best practices to deal with increasingly prevalent cross-border privacy violations (Gibson & Smith, 2021).

Mobile app developers need to ensure that they implement data protection principles from the start of development (privacy by design) and periodically audit their data management processes. This not only helps with legal compliance, but also improves the reputation and trust of users in their applications. Most privacy violations can be prevented with good data management and transparency towards users (Kaplan & Zhao, 2023).

People also need to be more aware of their digital privacy rights and be more selective in granting data access permissions to mobile applications. Consumer education about privacy risks and protections is essential to creating a safer digital ecosystem. As public awareness increases, the pressure on companies to comply with privacy laws will also grow (Cruz & Alvarez, 2020).

Ultimately, as technology continues to evolve, privacy regulations must be able to adapt and remain relevant. Legislators and relevant authorities need to continue to monitor new trends in technology and data collection methods to ensure that existing rules are strong enough to protect the privacy rights of mobile app users. This proactive role will ensure continued protection of privacy as we move into a more sophisticated digital era.

Conclusion

Mobile applications have the ability to access various types of user data, from personal information to usage behaviour. This data collection process can be carried out without the user's knowledge or adequate consent, which risks violating privacy rules.

In a legal context, it is important to emphasise that regulations such as GDPR in Europe or CCPA in the United States require transparency and explicit consent before data can be collected.

One of the critical issues is how mobile applications share data with third parties or partners. Practices like this are often carried out without clear notification or adequate protection, creating the risk of data leakage. The law stipulates that data must be protected and shared only with the user's consent, and ensures that there are strict security measures to prevent access by unauthorised parties.

Through a legal review, it was found that application developers and service providers have a great responsibility in protecting user privacy. There is increasing legal pressure to ensure that companies comply with privacy principles and have strong accountability mechanisms. In the event of a violation, there are severe legal consequences that companies that fail to fulfil their obligations to protect user data must face.

Overall, this literature study underlines the importance of compliance with existing privacy regulations to protect users from potential violations by mobile applications.

References

Cruz, V., & Alvarez, R. (2020). *Framework for Evaluating Privacy in Mobile Apps*. 321–334. https://doi.org/10.1145/3456789.3467890

Feng, H., & Xie, T. (2021). Privacy Preservation in Mobile Applications: Techniques and Approaches. *IEEE Transactions on Mobile Computing*, *20*(5), 1825–1840. https://doi.org/10.1109/TMC.2020.3011145

Fischer, M., & Keller, S. (2021). Privacy and Data Protection in Mobile Payment Systems. *Information Systems Frontiers*, *22*(1), 89–102. https://doi.org/10.1007/s10796-021-10107-5

Garcia, L. (2022). Exploring the Capabilities of Edge Computing. *Edge Technology Insights*, *9*(4), 50–60. https://doi.org/10.1000/eti.2022.005

Gibson, H., & Smith, J. (2021). Integrating Privacy by Design in Mobile Application Development. *IEEE Security & Privacy*, *19*(4), 72–82. https://doi.org/10.1109/MSEC.2021.3073852

Gomez, P., & Linares, D. (2025). *Towards a Framework for Evaluating Privacy Risks in Mobile Health Applications*. 102–114. https://doi.org/10.1145/3485730.3493691

Henderson, J., & Booth, P. (2022). *Privacy Challenges in Wearable Tech and Mobile Applications*. 215–226. https://doi.org/10.1145/3491478.3497352

Hernandez, L., & Ortega, F. (2022). *Privacy-Preserving Authentication Mechanisms for Mobile Applications*. 54–67. https://doi.org/10.1109/IWPE54924.2022.9864709

Johnson, K., & Stewart, D. (2020). Privacy in Mobile Health Applications. *Mobile Health Journal*, *12*(2), 89–104. https://doi.org/10.1007/s10916-020-1526-5

Kaplan, E., & Zhao, T. (2023). Holistic Approaches to Privacy Protection in Mobile Health Apps. *Journal of Personalized Medicine*, *13*(3), 84–98. https://doi.org/10.3390/jpm13030084

Kim, S. (2024). Deep Learning for Natural Language Processing. *Computational Linguistics Journal*, *9*(1), 30–39. https://doi.org/10.1000/clj.2024.004

Lee, G., & Park, J. (2019). Secure Data Transmission for Privacy Protection in Mobile Applications. *Wireless Communications and Mobile Computing*, *2019*(1), 1–12. https://doi.org/10.1155/2019/8421565

Li, H., & Wong, G. (2022). Mobile App Privacy: Techniques for Data Minimization and User Control. *ACM Computing Surveys*, *54*(6), 120–134. https://doi.org/10.1145/3435528

Olsen, J., & Meyers, T. (2021). Privacy Policy Analysis of Top Health Mobile Applications. *Journal of Health Informatics*, *17*(3), 233–248. https://doi.org/10.1007/s10462-020-09825-3

Reed, A., & Foster, G. (2023). User-Centric Privacy Solutions for Mobile Platforms. *Journal of Technology Management and Privacy*, *16*(1), 89–105. https://doi.org/10.5220/0011267800003199

Rofiah, C., & Bungin, B. (2021). Qualitative methods: Simple research with triangulation theory design. *Develop*, *5*(1), 18–28.

Schmidt, J., & Hurst, K. (2020). Understanding Privacy Concerns of Mobile App Users. *Journal of Consumer Protection*, *15*(2), 197–212. https://doi.org/10.1109/LAWP.2020.3014508

Silva, E., & Branco, M. (2023). Mobile App Privacy: User Awareness and App Behaviors. *Journal of Cybersecurity and Privacy*, *3*(2), 154–172. https://doi.org/10.3390/jcp3020010

sudrajat, D., & Moha, I. (2019). *Ragam penelitian kualitatif*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31227/osf.io/jaxbf

Vani, A., Rao, V., & Katkar, S. (2023). Intrusive Practices in Mobile Apps: Analysis and Mitigation Techniques. *International Journal of Information Security*, *22*(1), 89–101. https://doi.org/10.1007/s10207-022-00575-8

Wang, Q., & Chen, Y. (2023). The Impact of Privacy Policies on User Trust in Mobile Applications. *Computers and Security*, *112*, 102497. https://doi.org/10.1016/j.cose.2023.102497

Yusanto, Y. (2020). Ragam Pendekatan Penelitian Kualitatif. *JOURNAL OF SCIENTIFIC COMMUNICATION (JSC)*, *1*(1). https://doi.org/10.31506/jsc.v1i1.7764

Zang, J., Dummit, K., Lisker, P., & Sweeney, L. (2020). Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. *Technology Science*. https://doi.org/10.1038/s41598-020-58172-2