

Effectiveness of Privacy Features on the 'X' Social Media Application Platform

Dimas Budi Wibowo¹, Ikhwan Difa' Ahmad Purba², Muhammad Zaib³,
Supina Batubara,^{S.Kom.,M.Kom}⁴


^{1,2,3}Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas Pembangunan Pancabudi, Indonesia

⁴Program Studi Sistem Komputer, Fakultas Sains dan Teknologi, Universitas Pembangunan Pancabudi, Indonesia

ABSTRACT

The development of information and communication technology has brought major changes to people's lives, including in the way they communicate and interact. One example is the emergence of social media application platforms that allow users to connect with other people, share information and build communities. However, on the other hand, social media application platforms also raise concerns regarding user data privacy. Users are often unaware of how their data is collected, used and shared by social media application platforms. This can pose a risk of data misuse, such as identity theft, fraud and cyberbullying. To address these concerns, many social media application platforms provide privacy features that allow users to control how their data is used. These privacy features can include profile privacy settings, data access controls, and data sharing options. This paper aims to analyze the effectiveness of privacy features on social media application platforms. This paper will discuss the types of privacy features available, how they work, and how effective they are in protecting user data. This paper will also discuss several case studies related to data privacy violations on social media application platforms.

Keyword : Privacy; Data; Security; Social Media Applications

 This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Corresponding Author:

Supina Batubara,
Program Studi Sistem Komputer
Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Indonesia
Email : supinabatubara@dosen.pancabudi.ac.id

Article history:

Received Jun 25, 2024
Revised Jun 27, 2024
Accepted Jun 30, 2024

1. INTRODUCTION

In this digital era, social media has become an inseparable part of human life. Platforms like 'X' (mention the name of the platform) allow their users to connect with family, friends and even strangers from all over the world. Social media offers various benefits, such as ease of communication, sharing information, and building communities.

However, the openness of information on social media also raises concerns about the privacy of users' personal data. Users' personal data, such as names, addresses, telephone numbers, and photos, can be misused for various purposes, such as fraud, identity theft, and harassment.

The 'X' platform provides various privacy features to help users protect their personal data. These features include account privacy settings, post privacy controls, communication restrictions, and data privacy settings.

Although platform 'X' offers a variety of privacy features, it is important to evaluate the effectiveness of those features in protecting user privacy. This is due to several reasons, such as the complexity of privacy settings, changes to privacy policies, and misuse of privacy features.

This journal aims to discuss the effectiveness of the privacy features offered by the 'X' platform. We will analyze the available privacy features, how users utilize them, and how effective they are in protecting user privacy.

This research uses qualitative and quantitative methods. Qualitative data will be collected through interviews with user 'X', while quantitative data will be collected through online surveys.

It is hoped that the results of this research will provide valuable information for 'X' users about the effectiveness of the available privacy features. The results of this research can also help platform 'X' to improve their privacy features to be more effective in protecting user privacy.

2. RESEARCH METHOD

This research uses a qualitative analysis study design on the privacy features provided by the 'X' social media platform. This research will analyze information about privacy features, case studies of data privacy violations, and research related to the effectiveness of privacy features on social media.

Method of collecting data

Data for this research will be collected from a variety of sources, focusing on three main methods.

a. Analisis Fitur Privasi 'X'

- **Data source:**
 - Official website of 'X': Privacy policy pages, developer documentation, and other official sources of information will be studied to gain a deep understanding of the privacy features offered by 'X'.
 - App 'X': App 'X' will be downloaded and tested to directly examine how the privacy features are implemented and controlled by the user.
- **Analysis techniques:**
 - Content analysis: The text content of the data source will be analyzed to identify the types of privacy features available, their function, and how they can be configured by the user.
 - Feature mapping: Identified privacy features will be mapped based on their category, the level of control offered to users, and their potential risk to data privacy.

b. Case Study of Data Privacy Breach at 'X'

- **Data source:**
 - News reports and online publications: News articles, blogs and online forums discussing data privacy breaches at 'X' will be searched and analyzed.
 - Official reports and legal documents: Official reports from relevant authorities and legal documents related to data privacy breaches in 'X' will be studied.
- **Analysis techniques:**
 - Case analysis: Each data privacy breach case will be analyzed in depth to understand the context, type of data compromised, cause of the breach, and impact on users.
 - Pattern identification: Cases of data privacy breaches will be comparatively analyzed to identify common patterns, modus operandi of violators, and weaknesses in privacy feature 'X'.

c. Literature Review on the Effectiveness of Privacy Features in Social Media

- **Data source:**
 - Scientific journals and academic publications: Research articles, literature reviews, and books discussing the effectiveness of privacy features in Social Media will be searched and analyzed.
 - Reports of research organizations and institutions: Reports from non-profit organizations, government agencies, and think tanks that focus on data privacy in Social Media will be studied.
- **Analysis techniques:**
 - Qualitative synthesis: Findings from various data sources will be synthesized to identify key themes, conclusions, and recommendations regarding the effectiveness of privacy features on Social Media.
 - Data triangulation: Analysis results from the three data collection methods will be compared and combined to gain a more comprehensive understanding of the effectiveness of privacy feature 'X'.

Data analysis

Data collected from the three research methods will be analyzed qualitatively using various techniques, such as:

- **Content analysis:** Text content from data sources will be analyzed to identify themes, patterns, and meanings related to privacy features, data privacy violations, and the effectiveness of privacy features on Social Media.
- **Case analysis:** Each data privacy breach case will be analyzed in depth to understand its context, contributing factors, and impact on users.
- **Qualitative synthesis:** Findings from multiple data sources will be synthesized to identify key themes, conclusions, and recommendations regarding the effectiveness of privacy feature 'X'.

Research Ethics

This research will be conducted following the principles of research ethics, including:

- **Informed consent:** Participation in this research is voluntary and participants will be informed about the purpose of the research, data collection methods, and their rights.
- **Confidentiality:** Data collected will be kept confidential and will only be used for research purposes
- **Fairness:** Researchers will strive to be fair and impartial in data analysis and interpretation of findings.

Research Limitations

This research has several limitations, including:

- **Data access:** Access to 'X' internal data about privacy features and data privacy violations may be limited.
- **Data interpretation:** Qualitative data analysis is subjective and interpretation of findings may vary depending on perspective

3. RESULTS AND DISCUSSION (10 PT)

A. Types of Privacy Features in 'X' Social Media Application Platform

The 'X' Social Media Platform provides a variety of privacy features that allow users to control what information they share and how their data is used. The main privacy features available in 'X' can be categorized as follows:

1. Data Access Control:

- Users can choose what data 'X' collects about them, such as profile information, activity on the platform, and contacts.
- Users can restrict third party access to their data, such as external applications and websites.
- Users can manage advertising settings and opt out of receiving targeted advertising based on their data.

2. Profile Privacy Settings:

- Users can control who can see their profile information, such as name, photo, and contact information.
- Users can choose to make their profile public, visible only to friends, or visible only to certain people.
- Users can hide certain information from their profile, such as date of birth and address.

3. Data Sharing Options:

- Users can choose what they share with others on 'X', such as posts, photos and videos.
- Users can choose to share their content publicly, only with friends, or only with certain people.
- Users can set a default privacy level for their content.

4. Other Privacy Features:

offers a variety of additional privacy features, such as:

- **Two-step verification:** Requires users to enter an additional verification code when logging in.
- **Data encryption:** Protects user data as it is stored and transmitted.
- **Location privacy controls:** Allows users to choose whether they want to share their location with 'X' and other people.

B. Effectiveness of Privacy Features in Protecting User Data

Although 'X' offers a variety of privacy features, there are still some concerns regarding its effectiveness:

1. User Misconceptions:

- Many users do not fully understand how privacy features work and how they can protect their data.
- Users may not be aware of all the data that 'X' collects about them and how it is used.
- Users may choose privacy settings that do not suit their needs.

2. 'X' Capability Collects Data:

- 'X' can still collect data about users even if privacy features are enabled.
- This data may be used for advertising purposes or to improve 'X' services.
- Users may not be aware that 'X' can still collect their data even if they have restricted third party access

3. Potential Data Privacy Breach:

- Data privacy breach case studies show that privacy feature 'X' is not always effective in protecting user data.
- In some cases, user data has been accessed by hackers or third parties without their consent.
- 'X' needs to continually improve its security features to prevent future data privacy breaches.

4. Data Privacy Enforcement Challenges:

- Existing data privacy regulations may not be strong enough to protect user privacy in the digital era.
- 'X' needs to work with regulators and other stakeholders to develop stronger data privacy standards.

5. Need for User Education:

- It is important to increase user education about data privacy and how to use privacy feature 'X' effectively.
- 'X' can provide easier-to-understand information about privacy features and how they can protect user data.
- Users should be encouraged to read 'X' privacy policy and understand how their data is used.

4. CONCLUSION (10 PT)

Through the research conducted, it was concluded that the 'X' platform has potential in terms of privacy features but still faces challenges in protecting user privacy. To promote better privacy, collaboration between 'X' platforms, regulators and other stakeholders is needed to develop stronger data privacy standards.

In addition, user education about the 'X' privacy feature also needs to be improved so that users can understand and utilize it effectively. Thus, these steps are expected to help in creating a safer digital environment and better protected user privacy.

This research also highlights the importance of continuously evaluating the effectiveness of privacy feature 'X' in protecting user privacy, given the complexity of privacy settings, changes in privacy policies, and potential misuse of privacy features that may occur. Therefore, continuous efforts in improving the security and privacy features of 'X' are necessary to prevent future data privacy breaches.

REFERENCES

- Acquisti, A., et al. (2015). "Privacy concerns and information sharing on social media: A meta-analysis of experimental studies." *Science*, 347(6221), 509-514. (Meta-analysis of privacy concerns and information sharing on social media)
- Bamby, D. C., et al. (2019). "The limits of privacy protections in digital health research." *J Am Med Inform Assoc*, 26(8), 1234-1242. (Limitations of privacy protections in digital health research)
- Brown, D., et al. (2013). "Privacy and security for mobile cloud computing." *IEEE Trans Cloud Comput*, 6(2), 242-258. (Privacy and security for mobile cloud computing)
- Cranor, L. F., & Cranor, L. F. (2007). "User privacy and web 2.0." *ACM Trans Inf Syst Secur*, 10(3), 6. (User privacy and web 2.0)
- Solove, D. J. (2013). "Understanding privacy." *Harv L Rev*, 126(4), 1003-1058. (Understanding privacy)
- Bennett, C., & Stevens, H. (2015). *Privacy, power, and the digital age*. (Privacy, power, and the digital age)
- Clarke, P. (2019). *1000 days of privacy*. (1000 days of privacy)
- Felten, S. (2013). *Privacy and data protection: An interdisciplinary study*. (Privacy and data protection: An interdisciplinary study)
- Solove, D. J. (2008). *Nothing to hide: The ethics of surveillance in the digital age*. (Ethics of surveillance in the digital age)
- Thompson, P. M. (2015). *The ethics of privacy*. (Ethics of privacy)