JURNAL PSIKOLOGI:
Jurnal Ilmiah Fakultas Psikologi Universitas Yudharta Pasuruan
p-ISSN: 2088-0634; e-ISSN: 2715-6206
Vol. 13, No. 1, Maret 2026, 39-51

Digital Privacy and Netizens' Reactions to Obscene Videos: Perspectives from Cyberpsychology and Law

Ulfa Dyah Mustika[1*], Galih Setyo Refangga[2], Sri Wiworo Retno[3], Sigit Budi Santoso[4]
[1,3]Faculty of Psychology, Universitas Wisnuwardhana Malang
[2,4]Faculty of Law, Universitas Wisnuwardhana Malang
Corresponding author: [1*]ulfadyah@wisnuwardhana.ac.id

Abstract
This study aims to analyze netizens' responses to a case involving an indecent video featuring a teacher from a cyberpsychology perspective and to examine the associated criminal law implications. The study employed a descriptive qualitative approach, utilizing data collection techniques such as digital observation, unstructured interviews, and documentation. The study's informants consisted of ten individuals selected through purposive sampling based on their involvement in accessing, following, or responding to information related to the case under investigation. Data were analyzed using the interactive model of Miles, Huberman, and Saldaña through the stages of data condensation, data presentation, and drawing conclusions. The results indicate that netizens' responses are not homogeneous but encompass empathetic responses, victim-blaming, passive consumption, and content-saving practices. Although most informants understood the importance of digital privacy, this understanding is not always accompanied by behavior that supports privacy protection. This study also found a gap between normative legal awareness and understanding of the legal protection mechanisms available to victims. Furthermore, netizens' involvement occurs not only through the act of sharing information but also through activities such as accessing, saving, and following case developments, which contribute to the continued exposure of victims in the digital space.

Keywords: *criminal law, cyberpsychology, digital privacy, digital revictimization, public reaction*

Introduction

Advances in information and communication technology have transformed the way people interact, access information, and build social relationships in the digital space. The rise of social media platforms such as X (Twitter), Instagram, TikTok, and Facebook has enabled rapid, widespread, and geographically unrestricted dissemination of information. On the one hand, these developments have facilitated the exchange of information and public participation. On the other hand, however, advancements in digital technology have also increased the risk of violations of individual privacy. Information that was previously private can now be easily documented, disseminated, and consumed by the public without the owner's consent. Consequently, the boundary between private and public spaces has become increasingly blurred, posing new challenges to the protection of individual rights in the digital age.

Digital privacy is receiving increasing attention in both academic research and public policy. Advances in Internet-based technology, social media, and artificial intelligence have heightened the risk of personal data misuse and the dissemination of sensitive information that could harm individuals. Alshehri (2024) explains that modern digital privacy theory no longer focuses solely on the protection of personal data but also

considers user behavior, decision-making, and the social consequences arising from the use of personal information in the digital space. Furthermore, Böhm et al. (2024) found that concerns regarding digital privacy encompass the dimensions of control, exposure, and consequences experienced by individuals when their personal information is disseminated in the digital public sphere. Lutz's (2025) research also indicates that practices and understanding of digital privacy are influenced by social, cultural, technological, and regulatory factors within a given society. These findings suggest that digital privacy is a multidimensional phenomenon that cannot be understood solely as a technological issue but also as a social, psychological, and legal one.

An understanding of digital privacy cannot be separated from the concept of privacy as an individual's control over personal information. Solove (2008) explains that privacy violations are not only related to access to personal data but also encompass the dissemination, use, and exposure of information that may cause harm to individuals. In line with this, Nissenbaum (2010), through the concept of contextual integrity, asserts that information is considered a privacy violation when it is used or disseminated outside its proper social context. This perspective is relevant for understanding the dissemination of explicit videos on social media because private information is transformed into public consumption without the consent of the parties involved. A common form of digital privacy violation is the dissemination of non-consensual intimate content. This phenomenon becomes increasingly complex when the disseminated content involves public figures or individuals in specific professions who hold strategic social positions. In 2024, the Indonesian public was confronted with the dissemination of an indecent video involving a teacher that went viral across various social media platforms. The case sparked a wide range of reactions from the netizens. While some members of the public have shown empathy and support for the victim, others have engaged in victim-blaming, sharing videos, or turning the case into digital entertainment. This situation demonstrates that the spread of sensitive content in the digital sphere is influenced not only by the actions of the primary perpetrators but also by the collective involvement of social media users, who amplify the reach and impact of such content.

Cases involving educators have distinct characteristics compared to similar cases involving the general public. Teachers are viewed not only as individuals but also as educational figures who are socially associated with moral values, integrity, and exemplary conduct. Therefore, when a privacy violation involving an educator occurs, the public response often focuses not only on the violation itself but also on the professional identity associated with that individual. Consequently, the digital space becomes an arena for moral judgment that can reinforce social stigma, victim-blaming, and digital revictimization. This situation makes it important to examine cases involving educators because they demonstrate how digital privacy, public morality, and professional identity interact in shaping public responses in cyberspace.

From a cyberpsychology perspective, netizens' behavior in responding to an event on social media is influenced by the characteristics of online interactions, which differ from those of face-to-face interactions. According to Mustika et al. (2025), cyberpsychology is a branch of psychology that studies the reciprocal relationship between humans and digital technology, including how cyberspace influences the

cognitive processes, emotions, behavior, identity, and social interaction patterns of Internet users. In the context of social media, cyberpsychology helps explain how the characteristics of digital technology shape both individual and collective societal behavior when facing a viral event. One key concept in cyberpsychology is the online disinhibition effect proposed by Suler (2004), which refers to the tendency of individuals to express thoughts, emotions, or certain behaviors more freely in an online environment. Although this theory remains relevant, recent research indicates that digital behavior is influenced not only by anonymity, but also by platform design, algorithms, group norms, and the dynamics of information virality.

Wright et al. (2025) found that social media users' comments on cases involving sexual issues are still dominated by victim-blaming and moral judgment, which exacerbate the victims' situation. Wu et al. (2025) showed that users' decisions to share information on social media are often influenced by emotional factors, curiosity, and a desire to engage in trending conversations. These findings indicate that netizens' behavior in the digital space is not always based on ethical or legal considerations, but is also influenced by psychological mechanisms that develop within the digital environment. In line with this, Mustika et al. (2025) explain that cyberspace enables the formation of a "cyberself," which is a self-representation constructed through digital activities. In certain situations, individuals may exhibit different behaviors in digital spaces than when interacting in person. This helps explain why some netizens can easily engage in social judgment, victim blaming, or the dissemination of sensitive content without considering the psychological impact on the victim.

On the other hand, from a legal perspective, Indonesia already has various instruments governing digital privacy protection, including Law No. 27 of 2022 on Personal Data Protection and Law No. 1 of 2024 on the Second Amendment to the Law on Electronic Information and Transactions. The existence of these regulations demonstrates the state's commitment to protecting the public's right to privacy in the digital space. However, various cases of dissemination of personal content continue to occur, indicating that the regulations have not yet been fully effective in preventing digital privacy violations. Firdaus and Wardhani (2025) explain that the primary challenge in personal data protection in Indonesia lies not only in regulatory aspects but also in the public's low digital literacy and legal awareness. Thus, the effectiveness of legal protection for digital privacy cannot be separated from the behavior of social media users as part of the digital ecosystem itself.

Various previous studies have made significant contributions to our understanding of digital privacy, social media user behavior, and legal protection in cyberspace. Research by Alshehri (2024), Böhm et al. (2024), and Lutz (2025) enriches our understanding of the concept of digital privacy and the factors that influence user behavior in managing personal information. Meanwhile, Wright et al. (2025) highlight the phenomenon of victim-blaming in social media comments, while Wu et al. (2025) explain the role of emotional factors and virality in the dissemination of information in the digital space. Nevertheless, most of these studies have focused on specific aspects of isolation. Digital privacy studies tend to emphasize data security and control over personal information, whereas cyberpsychology research primarily explains user behavior without linking it to its potential legal consequences. Furthermore, research on

victim blaming generally focuses only on public comments or perceptions of victims, thus failing to sufficiently address the involvement of users acting as spectators, savers, or re-consumers of sensitive content—roles that also have the potential to prolong the impact of privacy violations.

Previous research has generally focused on those who disseminate content or engage in victim-blaming practices on social media platforms. In reality, netizens' responses to cases of digital privacy violations can take various forms of engagement, such as accessing, saving, following developments in the case, or commenting on circulating information. These diverse forms of engagement indicate that digital privacy violations are influenced not only by the primary perpetrators of the dissemination but also by the broader participation of social media users.

Based on this review, a gap remains in the literature regarding the relationship between digital privacy, netizen responses, and criminal law implications within a comprehensive analytical framework. Previous research has not extensively examined how various forms of netizen engagement, such as disseminators, storers, viewers, or commenters, can contribute to the process of digital revictimization and influence the effectiveness of privacy protection for victims. This research gap becomes increasingly significant when the cases under study involve the teaching profession, which holds a socially strategic position as an educational figure and moral role model in society. Therefore, research that can integrate the perspectives of cyberpsychology and criminal law is needed to understand this phenomenon more comprehensively. The cyberpsychology approach, as described by Mustika et al. (2025), is important because it allows for the analysis of psychological factors that drive netizens' involvement in the dissemination, storage, or reconsumption of sensitive content, whereas the criminal law perspective is necessary to examine the legal implications of such behavior on the protection of victims' privacy.

Based on the above discussion, this study aims to analyze netizens' responses to a case involving the dissemination of an indecent video featuring a teacher, understand how the public perceives digital privacy in this context, and examine the implications psychological and criminal law regarding the protection of victims' privacy in the digital space. The contribution of this study lies in the integration of cyberpsychology and criminal law perspectives to explain netizens' involvement in the process of digital revictimization. Furthermore, this study expands the discussion on digital privacy violations by highlighting not only the behavior of content dissemination but also the behaviors of viewing, saving, and commenting on content as part of the mechanisms that can prolong the impact of privacy violations in cyberspace.

Method

Research Design

This study employs a qualitative approach with a descriptive-interpretive design to understand netizens' responses to a case involving an indecent video featuring a teacher, as well as its implications for digital privacy, cyberpsychology, and criminal law.

Participants

The research was conducted online from July to September 2025 through digital observation on platforms X (Twitter), Instagram, TikTok, and Facebook, which served as the primary spaces for public discussion regarding the case. Informants were selected using purposive sampling with the following criteria: (1) active social media users aged 15–50 years; (2) those who had viewed, saved, shared, or commented on the case under study; and (3) those willing to serve as research informants. Based on these criteria, ten informants with diverse characteristics and digital experiences were recruited.

Measures

Research data were collected through digital observations, unstructured interviews, and documentation in the form of screenshots, posts, and comments relevant to the research focus. Observations were conducted non-participatively; that is, the researcher did not engage in the observed interactions but instead focused on patterns of response and forms of netizen participation regarding the case under study.

Data Analysis

Data analysis utilized the interactive model proposed by Miles et al. (2014), which includes data reduction, data presentation, and drawing conclusions and verification. Data validity was strengthened through source and methodological triangulation by comparing the results of the observations, interviews, and documentation obtained during the study.

Results

Characteristics of the Research Informants

This study involved ten informants selected using purposive sampling based on their engagement with information and discussions related to the case of an indecent video involving a teacher on social media. The informants consisted of six men (60%) and four women (40%) aged 15–50 years. All informants were active social media users who regularly accessed digital platforms and were exposed to information regarding the case study.

Table 1.
Characteristics of Research Informants

Respondent code	M/F	Age	Platform	Dominant role in content
R1	M	24	X	Saver
R2	F	19	IG	Empathetic Commenter
R3	M	30	X	Reposter
R4	F	26	Tiktok	Mixed Commenter
R5	M	22	Tiktok	Victim-Blaming Commenter
R6	M	34	X	Passive Viewer
R7	M	28	FB	Saver for Personal Use
R8	F	20	X	Viewer and Saver
R9	M	41	X	Saver and Reposter
R10	F	37	IG	Empathetic Commenter

Based on the characteristics of the informants, the majority of respondents were active social media users who accessed various digital platforms daily. X (Twitter),

Instagram, TikTok, and Facebook are the most frequently used platforms for obtaining information and following developments on trending issues. These characteristics indicate that the informants had a high level of exposure to various forms of digital interaction, thereby providing insight into how netizens respond to cases of indecent videos involving a teacher.

Forms and Patterns of Netizens' Responses to the Indecent Video Case

The results of digital observations conducted on X, Instagram, TikTok, and Facebook show that discussions regarding the indecent video case involving a teacher are dominated by a diverse range of public responses. The comments found not only expressed support for the individuals in the video but also included moral judgments, intense curiosity about the video's content, and calls to seek out and access circulating material. Additionally, posts that indirectly encouraged other users to continue following the case's developments were identified. These observational findings were subsequently corroborated by the results of the interviews with informants. The interview results showed that some of the informants responded empathetically to the individuals featured in the video. This group viewed the distribution of the video without consent as a violation of privacy that could have psychological, social, and reputational consequences for the victims. One of the informants stated that *"yang salah itu yang menyebarkan, tetapi orang-orang justru lebih fokus pada isi videonya daripada dampak yang dialami orang yang ada di dalam video"* (R2). Another informant also argued that the individuals in the video still have a right to privacy, even though the content has been widely circulated on social media. According to this informant, *"kalau videonya tersebar tanpa izin, yang harus dipermasalahkan itu penyebarannya, bukan orang yang ada di dalam videonya"* (R3).

On the other hand, this study also found responses that pointed toward victim-blaming. Some informants believed that the individuals in the video shared responsibility for the consequences that arose after the video was shared. One informant stated that *"kalau dari awal tidak membuat video seperti itu mungkin tidak akan terjadi masalah sebesar ini"* (R6). Another informant revealed that the public tends to pass judgments based on prior actions, leading to the perception that the victim has contributed to the problem (R10). This finding indicates that some netizens still link privacy violations to moral judgments of victims.

In addition to these two types of responses, a group of informants was identified that could be categorized as passive consumers. This group is not involved in spreading or commenting on the circulating case but continues to actively follow developments through various social media platforms. One informant explained that they were only following the case because the topic was trending and did not feel the need to comment on or repost the information they received. This informant stated that *"saya hanya melihat saja karena memang sedang ramai dibahas, saya tidak ikut komentar atau membagikan"* (R4). Another informant said that they were following the case to stay informed about the information circulating without feeling the need to get involved in public discussions on social media (R1).

Another notable finding is that some informants admitted to saving circulating content without intending to redistribute it. Most informants who engaged in this behavior attributed it to curiosity and the desire to understand the context of the events

more fully. One participant explained that they saved the video out of concern that the content might have been deleted before they could grasp the full story unfolding on social media. According to that informant, *"saya simpan karena penasaran dan takut nanti videonya hilang sebelum tahu cerita lengkapnya"* (R8). Another informant also acknowledged that saving content was done for personal reasons and was not intended to be shared with other users (R5). Overall, the research findings indicate that netizens' engagement with cases involving indecent videos occurs not only through the act of reposting information but also through activities such as watching, saving, following case developments, and commenting. These various forms of engagement indicate that the dissemination of sensitive content in the digital space involves broader participation than the primary actors who first shared the content.

Netizens' Understanding of Digital Privacy

The interview results show that all informants have a basic understanding of the concept of digital privacy. Most researchers define digital privacy as an individual's right to control personal information and determine who can access it. One informant explained that privacy is a person's right to prevent personal information from being disseminated without permission. According to that informant, *"privasi itu hak seseorang untuk menjaga hal-hal pribadi supaya tidak disebarkan sembarangan"* (R1). Another informant also stated that personal information should only be accessible to parties who have obtained permission from the owner (R7).

Nevertheless, this study found that an understanding of the importance of digital privacy is not always accompanied by a behavior that supports privacy protection. Some informants who stated that sharing videos without permission is wrong still accessed or saved circulating content. When asked about their reasons for doing so, curiosity was the most cited factor. One informant admitted that they understood that action was not entirely right but were still compelled to view the content because they wanted to know what was actually happening. The informant stated that *"sebenarnya saya tahu itu bukan hal yang baik, tetapi saya penasaran karena semua orang membicarakannya"* (R5). Another participant also noted that curiosity is often stronger than the desire to avoid information that is going viral on social media (R8). These findings suggest that a conceptual understanding of digital privacy is not always accompanied by digital practices that are consistent with privacy protection principles. In other words, awareness of the importance of privacy is not fully reflected in users' behavior when faced with content that captures public attention.

Netizens' Understanding of Legal Implications

The research findings indicate that most informants are aware that the dissemination of private videos without consent can have legal consequences. However, their understanding of the available forms of legal protection remains relatively limited. Most informants only generally know that the distribution of personal content can result in legal sanctions, but do not understand in detail the reporting mechanisms or the rights of victims that can be invoked when a digital privacy violation occurs. When asked about the reporting procedures or forms of legal protection available to victims, most informants were unable to provide a clear explanation. One informant stated that *"saya tahu itu bisa kena hukum, tetapi kalau ditanya pasal atau cara melaporkannya saya tidak tahu"* (R7). Another informant also mentioned that they had heard of the Electronic

Information and Transactions Law but did not yet understand how those regulations are applied in cases of the dissemination of private videos. According to that informant, *"saya pernah dengar soal UU ITE, tetapi kurang paham kalau untuk kasus seperti ini proses hukumnya bagaimana"* (R9).

In addition, some informants believed that legal consequences applied only to the person who first disseminated the video. They were unaware that sharing, aiding in dissemination, or expanding access to content that violates privacy can also result in certain legal implications. These findings indicate that netizens' legal awareness remains at a general level, that is, they know that an action is legally wrong but do not yet understand in detail the forms of protection available or the legal consequences that may arise from their involvement in the dissemination, storage, or consumption of sensitive content in the digital space. Thus, the results indicate that the public's understanding of digital privacy in the context of the cases studied is based more on moral considerations than on an understanding of the legal aspects governing it. This structure of understanding is one of the factors influencing how netizens respond to and participate in cases of privacy violations emerging on social media.

Discussion

Netizens' Reactions and the Spectrum of Digital Engagement in Privacy Violations

The research findings indicate that netizens' responses to the indecent video case involving a teacher were not uniform but fell across a spectrum of varying levels of engagement. Some informants expressed empathy toward the victim and viewed the distribution of the video without consent as an unjustifiable violation of privacy. Conversely, some informants exhibited a tendency toward victim blaming by attributing the video's distribution to the behavior of the individuals depicted in it. In addition to these two forms of responses, a group of netizens was also found who chose to be passive consumers by merely following the case's developments, as well as a group that saved the content without redistributing it. These findings indicate that netizens' involvement in digital privacy violations is far more complex than a simple categorization into perpetrators and non-perpetrators. Previous research has tended to focus on information dissemination and victim blaming as the primary forms of public response toward victims in the digital space (Wright, 2025; Ubino & Astuti, 2025). However, the results of this study show that the continuity of information dissemination is influenced not only by perpetrators who repost content but also by users who actively access, store, and follow the development of circulating content.

Findings regarding the practice of saving content out of curiosity indicate that netizens' engagement is not always driven by a desire to disseminate information, but also by a need to gain a more complete understanding of events that are going viral. Interestingly, the curiosity expressed by informants cannot be fully understood as neutral motivation. In the social media context, curiosity functions as a psychological mechanism that drives individuals to continue accessing content that is currently in the public spotlight even though they are aware that such content involves privacy violations. These findings suggest that virality is not only produced by digital platform algorithms but also by users' psychological need to obtain information deemed exclusive, sensitive, or currently at the center of public attention. From a

cyberpsychology perspective, this indicates that digital behavior is not always driven by the intent to harm others. Most informants attributed their engagement to curiosity, a desire to obtain more complete information, and the need to follow issues currently in the public spotlight. This finding is consistent with the research of Wu et al. (2025), who explain that the virality of information on social media is often influenced by emotional factors and individuals' need to stay connected to ongoing public conversations.

In the context of this study, curiosity serves as a driving factor that prompts individuals to continue accessing content even though they understand that the information involves privacy violations. Interestingly, some informants did not view the act of saving content as a form of involvement in a privacy violation. They believe that a violation only occurs when someone actively redistributes information to others. This finding indicates a discrepancy between individual perceptions and the social impact of such digital behavior. In fact, continued access to and storage of sensitive content by users helps sustain the content's existence in the digital space. Thus, this study demonstrates that digital privacy violations are perpetuated not only by active disseminators but also by a broader network of digital participation.

Digital Privacy and the Paradox of Netizen Behavior

These research findings indicate that all informants possess a basic understanding of digital privacy as an individual's right to control personal information and determine who can access it. Most informants also stated that the dissemination of personal videos without consent was wrong and unjustifiable. However, the findings suggest that this understanding is not always accompanied by behavior that is consistent with privacy protection principles. Some informants, while aware that the dissemination of videos without permission constitutes a privacy violation, still accessed, saved, or followed updates on the circulating content. This situation highlights the gap between normative understanding and daily digital practices. Informants recognize that privacy is a right that must be respected, but they have not yet connected their actions to a process that can prolong the privacy violations experienced by victims.

This phenomenon can be explained by the concept of the privacy paradox, which refers to a situation in which individuals express concern for privacy but still engage in actions that contradict the principles of privacy protection (Lutz, 2025; Connolly et al., 2025). However, the results of this study reveal a different dimension from that of previous research. While most previous studies have addressed the privacy paradox in the context of protecting internet users' personal data, this study demonstrates that the paradox also emerges in how individuals treat others' privacy. Individuals may view privacy as an important right to protect, yet simultaneously engage in activities that potentially contribute to the violation of others' privacy. Furthermore, the findings of this study suggest that social media users' decisions are not always based on ethical or legal considerations. Such behavior is also influenced by social and psychological factors, such as the desire to remain part of the public conversation, fear of missing out, and the urge to stay informed about trending issues. Under such circumstances, awareness of the importance of privacy is often overshadowed by the need to obtain information deemed relevant or of public interest. These findings suggest that the challenges of digital privacy protection are not limited to regulatory or technological aspects, but also involve fostering ethical awareness in the use of digital media.

Therefore, digital literacy needs to be developed not only to improve users' technical skills in safeguarding their personal data, but also to foster an understanding of the social and psychological consequences of consuming information that violates others' privacy. Thus, the protection of digital privacy depends not only on individuals' ability to protect themselves but also on their ability to respect the privacy of others in the digital space.

Digital Revictimization as a Consequence of Collective Participation

One of the key findings of this study is that the impact experienced by victims stems not only from the actions of the perpetrator who initially disseminated the video, but also from various forms of response that emerge in the digital space. Judgmental comments, victim-blaming, content storage, and repeated consumption of information contribute to the prolonged exposure experienced by victims. This finding indicates that digital space can serve as an arena for repeated and ongoing revictimization. Previous research has identified victim blaming as the primary form of secondary revictimization experienced by victims on social media (Ismarina, 2025; Ubino & Astuti, 2025). However, the results of this study indicate that digital revictimization has a broader scope. Victims not only face blaming or judgmental comments but also confront the reality that content violating their privacy continues to be searched for, saved, and consumed by other users. Digital revictimization occurs not only through language and social judgment but also through information consumption practices that perpetuate the existence of such content in the digital space.

These findings indicate that the line between perpetrators and audiences in the digital space is becoming increasingly blurred. Individuals who have never uploaded or reposted content can contribute to the perpetuation of privacy violations through consumption practices that maintain the social value of such content. In other words, digital revictimization is not only caused by active actions but also by passive participation that collectively creates demand for privacy-violating content. This interpretation suggests that victims' suffering does not end once the initial dissemination process is complete. Every new form of interaction with circulating content has the potential to prolong the psychological impact experienced by the victim. Therefore, in this study, digital revictimization is understood as a social process involving the collective participation of social media users and not merely the result of the actions of the individual who first disseminated the content.

Criminal Law Implications in Digital Privacy Protection

The research findings indicate that most informants are aware that the dissemination of private videos without consent can result in legal consequences. However, this knowledge remains general in nature and is not accompanied by an understanding of the mechanisms of legal protection or the legal consequences of their involvement in the dissemination of such information. These findings reveal a gap between normative and practical legal awareness. Informants know that the act of distributing videos is a violation of the law, but they do not understand how victims can obtain protection or how the acts of storing, reposting, or helping expand access to content can have specific legal implications. This situation indicates that the effectiveness of digital privacy protection is determined not only by the existence of regulations, but also by the public's level of understanding of applicable legal norms.

From a criminal law perspective, the existence of Law No. 27 of 2022 on Personal Data Protection and Law No. 1 of 2024 on Electronic Information and Transactions provides a sufficiently strong normative foundation for the protection of victims of digital privacy violations. However, research findings indicate that the primary challenge no longer lies in the availability of legal instruments, but rather in the public's low legal literacy regarding victims' rights and the legal consequences of their digital behavior. These findings suggest that regulations do not automatically lead to legal compliance in the digital space. The informants' limited understanding of victim protection mechanisms indicates that the preventive function of the law has not yet been fully realized. In this context, the main challenge is no longer the creation of new legal norms, but rather how existing norms can be understood, accepted, and internalized by social media users as guidelines for behavior in the digital space.

Furthermore, this study shows that netizens' involvement in cases of digital privacy violations occurs not only through sharing or commenting, but also through content storage, passive consumption, and monitoring case developments. These findings indicate that digital privacy violations occur within a broader participation network than has been widely discussed in previous research. Additionally, this study identified a gap between moral and legal awareness. Most informants understood that sharing a video without consent was wrong, but they did not fully grasp the victims' rights or the legal consequences of their involvement in accessing, storing, or helping spread the information.

Conceptually, this study demonstrates that digital privacy violations are not only the result of actions by the primary perpetrators who initially disseminate the content, but also stem from a spectrum of digital engagement involving disseminators, commenters, content savers, active observers, and passive consumers. This perspective broadens our understanding of digital privacy violations, which has traditionally focused on perpetrators of dissemination and victim-blaming. These findings indicate that protecting victims in the digital space requires attention not only to the primary perpetrators but also to information consumption practices that allow privacy-violating content to persist and continue circulating in cyberspace. This study demonstrates that digital privacy protection cannot be understood solely as a legal or technological issue. Digital privacy violations are multidimensional phenomena that simultaneously involve psychological, social, cultural, and legal aspects. Therefore, efforts to protect victims require a more integrative approach by strengthening digital literacy, raising legal awareness, optimizing law enforcement, and fostering a digital culture that is more empathetic toward victims. The findings of this study also expand our understanding of netizens' involvement in cases of digital privacy violations by demonstrating that the duration of the impact experienced by victims is determined not only by the primary perpetrators of content dissemination but also by various forms of digital participation by other social media users.

Conclusion

This study demonstrates that the dissemination of sensitive content on social media is a multidimensional phenomenon involving moral, social, digital-cultural, and legal aspects. Based on interviews with ten respondents, it was found that public

attitudes toward privacy violations remain diverse, ranging from empathy and support for victims to victim-blaming or consumption of the content out of curiosity. The findings also indicate that the public's awareness of digital ethics is not yet aligned with their legal awareness. Most respondents knew that the dissemination of personal content is prohibited, yet they did not understand the reporting mechanisms or agencies that can be contacted. This highlights the gap between normative law and social practices in the digital space. Overall, legal protection for digital privacy has not yet been substantively effective. Legal efforts must be complemented by improved digital literacy, education on online ethics, and platform policies that prioritize victims, so that the law is not merely a set of formal rules but is also embedded in the consciousness and behavior of the digital community.

References

Alshehri, A. (2024). A Review of Online Information Privacy Theories Advanced in Eight AIS Journals Over the Last Decade. *Information Resources Management Journal*, *37*(1), 1-22. https://doi.org/10.4018/IRMJ.349977

Böhm, G., Pfister, H. R., Ayres-Pereira, V., & Tjøstheim, I. (2024). E-privacy Concerns: A Facet Theoretical Approach. *Journal of Risk Research*, *27*(1), 1–20. https://doi.org/10.1080/13669877.2023.2288012

Connolly, L. Y., Lang, M., & Gibony, J. (2025). A Study of the Privacy Paradox Amongst Young Adults in the United Arab Emirates. *Telematics and Informatics Reports*, *19*(1). 100248. https://doi.org/10.1016/j.teler.2025.100248

Firdaus, A., & Wardhani, D. F. (2025). Protecting Privacy in the Digital Era: Personal Data Security in Indonesia. *Inovasi Pembangunan: Jurnal Kelitbangan, 13*(1), 1–16. https://doi.org/10.35450/jip.v13i1.915

Ismarina. (2025). Determinants of Victim Blaming among Students in Sexual Violence Cases: A Case Study at Faletehan University, Indonesia. *Contagion: Scientific Periodical Journal of Public Health and Coastal Health, 7*(1), 259–271. http://dx.doi.org/10.30829/contagion.v7i1.23802

Lutz, C., Baruh, L., Quinn, K., Epstein, D., Masur, P. K., & Wilhelm, C. (2025). Comparative Approaches to Studying Privacy: Introduction to the Special Issue. *Social Media + Society*, *11*(1), 1–14. https://doi.org/10.1177/20563051251344460

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Sage.

Mustika, U. D., Utami, W., & Widodo. (2025). Pemanfaatan Psikologi Forensik untuk Pencegahan Kekerasan Seksual Berbasis Elektronik antar -Warga Kampus. Maksigama, 19(1), 27-40.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, *7*(3), 321–326. https://doi.org/10.1089/1094931041291295

Ubino, S., & Astuti, K. (2025). The impact of victim blaming on social media and handling efforts for victims of sexual violence. *Research Horizon, 5*(4). https://doi.org/10.54518/rh.5.4.2025.758

Wright, E., Eriksson, L., & Bond, C. E. W. (2025). Victim Blaming, Gender, and Social Media Commentary: A Randomized Vignette Study of Audience Comments on News Reports of Intimate Partner Homicide. *Journal of interpersonal violence*, *41*(9-10), 1836–1863. https://doi.org/10.1177/08862605251322816

Wu, M., Wu, T., & Xiao, Y. (2025). Why people share misinformation on social media? An integration of affordance and flow theories. *Humanities and Social Sciences Communications*, *12*, 1129. https://doi.org/10.1057/s41599-025-05511-6