Now You See Me: Discussing Youth Privacy Paradox and Contextual Integrity in TikTok

Al Firdhausi, Mufti Nurlatifah
Universitas Gadjah Mada

Email: azmiiikfirdhausi@mail.ugm.ac.id,mufti.latifah@ugm.ac.id

Received January 3, 2025; Revised on March 9, 2025; Accepted November 25, 2025

Abstract
Privacy has emerged as a critical subject for media and communication research, especially with the youth's growing use of TikTok as a social networking site. This study aims to describe privacy among active young TikTok users through the perspective of the Contextual Integrity Privacy Theory by Helen Nissenbaum and the Privacy Paradox. This study adopts a qualitative research approach and a single case study. This research was analyzed through in-depth interviews with seven TikTok users aged 15-24. The findings reveal how youth navigate privacy concerns in their data practices, highlighting the role of contextual integrity in shaping their decisions. Participants demonstrated an acute awareness of privacy risks and employed strategies such as selective sharing, pseudonym use, and engagement with privacy tools to safeguard personal information. However, the study also highlights the persistence of the privacy paradox, where the desire for social validation often conflicts with privacy behaviors. These insights contribute to the theoretical discourse on privacy and offer practical recommendations for robusting safer and more transparent digital environments for youth.

Keywords: Paradox Privacy, Privacy Contextual Integrity, Social Networking Sites, TikTok, Youth

INTRODUCTION

Social networking sites have increasingly been used in youth's daily lives, serving as a room for digital interaction. Boyd and Ellison (2007) define social networking sites as web services that facilitate creating and maintaining social connections, including known and unknown individuals. Digital interaction allows youth to stay updated and maintain peer social networks (Kusumastuti, 2021). However, these communication norms (Siibak & Traks, 2019) have normalized sharing personal information, such as self-photographs, videos, and thoughts, posing significant privacy concerns. TikTok, as one of the emerging social networking sites, exemplifies the dual-edged nature of this trend. While offering new opportunities for connection and expression, TikTok also exposes vulnerabilities among youth. Nissenbaum's (2004; 2009) theory of Privacy Contextual Integrity highlights how technological advancement exacerbates privacy risks, especially for youth. The

phrase ‘Now You See Me’ captures the paradox youth face on TikTok, seeking visibility and connection while managing privacy practices in social networking sites as public digital space.

Youth, defined as individuals aged 15-24 years (Livingstone, 2019; UNICEF, 2013), are navigating a critical stage of identity information. Their high interaction on social networking sites often arises from a need for self-presentation and social validation, inadvertently exposing youth to privacy risks and threats. Livingstone (2019) has listed the risks as data exploitation and non-consensual content sharing from peers and strangers. Although youth are often perceived as indifferent to privacy, the stereotype could oversimplify the youth's behavior. Research suggests that youth may feel a sense of control over their data. Yet, they remain vulnerable to exploitation by social networking platforms that unilaterally decide data collection and sharing policies (Riyanto & Pratomo, 2023).

TikTok is a prime example, catering extensively to younger users and illustrating the tension between the desire for social validation and privacy concerns. TikTok has been at the center of significant privacy controversies. In 2023, TikTok recorded the highest global weekly usage, reflecting its significant role in the lives of youth (We Are Social, 2024). Investigations (EDPB, 2021) have revealed its practices of mismanaging consent for data collection and failing to protect underage profile accounts adequately. Despite ongoing efforts to enhance privacy safeguards, such as private account settings for users aged 13-15, privacy violations persist. Indonesia’s Cybersecurity Agency reports (BSSN, 2023) indicate widespread digital risks, with over 400 million anomalous cyber activities detected in 2023. These investigations catch violations, including unauthorized data sharing, bullying, grooming, and the non-consensual spread of private content (Saraswati, 2021). These alarming data underscore the urgent need to explore the privacy management strategies of TikTok’s youth users.

This study aims to understand how youth perceive and manage privacy on TikTok, employing Helen Nissenbaum’s Contextual Integrity Privacy Theory as a guiding framework. This theory helps examine how contextual norms shape an individual’s data-sharing decisions. Given TikTok’s popularity among youth and its extensive privacy policy, which spans 11,781 words (Roderick, 2020), it is a relevant case for exploring the dynamics.

Focusing on youth, a group particularly vulnerable to privacy risks, this research seeks to uncover the nuanced interplay between digital habits, contextual norms, and privacy concerns. The central research is: “How do youth understand and manage privacy contextual integrity in using TikTok?” This study enhances the

theoretical understanding of privacy while providing practical insights for creating safer digital environments for youth. Ultimately, it offers valuable guidance to practitioners and policymakers.

LITERATURE REVIEW

Privacy on social networking sites has become a significant concern in the context of technological advancements enabling rapid and wide dissemination of information. Despite general agreement on the importance of privacy, its meaning remains complex and challenging to define (Han, 2011). Social networking sites like TikTok, Facebook, and Instagram offer platforms for users to craft public profiles, connect with others, and share content. As described by Kuss and Griffith (2011), social networking sites are platforms where users craft public profiles, connect with friends, and engage with others who share similar interests. However, they also depend heavily on collecting data and using algorithms, which raises serious privacy concerns (Dwyer, 2011).

Theoretical Perspectives in Youth Privacy Studies

Research on youth privacy on social networking sites can be categorized into several main themes. First, the most prominent studies focus on how youth perceive privacy and the dynamics of managing self-disclosure on social networking sites (Trepte & Reinecke, 2011; Madden et al., 2013; Al Haidar, 2023). Second, privacy research seeks to identify and evaluate the challenges youth face in dealing with privacy issues arising from the everyday use of technology (Grodzinsky & Tavani, 2011; Fiesler & Proferes, 2018; Villebro et al., 2018). Third, research concentrates on regulatory studies on youth privacy in social networking contexts (Li et.al, 2019; Smirnova & Morales, 2024).

The existing literature reveals that research on youth privacy in social networking sites is predominantly framed within the theoretical perspective of Communication Privacy Management (CPM). This theory explores how individuals make decisions to disclose or conceal personal information based on criteria that distinguish private from public information based on criteria that distinguish private from public information and specific contextual conditions (Al Haidar & Tutiasri, 2023; Trninic & Vulkelic, 2021; Rinestu & Handayani, 2021; Thompson, 2021; Zhang & Fu, 2020; Barth & de Jong, 2017; Marwick, 2017; De Wolf, 2016). However, CPM theory has been criticized for inadequately addressing the complexities of privacy, which extend beyond individual issues to structural dimensions. Consequently, researchers increasingly turn to the Contextual Integrity Privacy Theory framework to address these broader concerns.

Studies employing Contextual Integrity Privacy Theory often adopt quantitative approaches, utilizing surveys as the primary data collection method. These studies aim to understand youth's perceptions of privacy in digital contexts and examine how these perceptions influence shared information management (Fiesler & Proferes, 2018; Madden et al., 2013). On the other hand, qualitative research using this theory frequently relies on secondary data through a literature review as the primary data collection method. These studies primarily explore how technology, particularly digital platforms, shapes and transforms privacy norms (Kumar et al., 2024; Malkin, 2022; Saraswati, 2021; Livingstone, 2019; Adorjan & Ricciardelli, 2019; Badilo et al., 2018; Balleys & Coll, 2017). Fewer studies employ mixed-method approaches, integrating quantitative and qualitative data collection techniques (Trepte & Reinecke, 2011; Grodzinsky & Tavani, 2011).

Based on earlier research findings, this research is positioned to address identified gaps. It employs Contextual Integrity Privacy Theory to explore youth privacy, focusing on the norms and contexts shaping their understanding, awareness, and decision-making in privacy practices. This theoretical framework offers a nuanced view of how TikTok, a prominent digital interaction platform among youth, contributes to forming privacy norms and contexts. This study adopts a qualitative approach to address the gaps identified in previous research, emphasizing an in-depth exploration of participant experiences. As the object of this research, TikTok represents a novel contribution to the field, given its unique characteristics and limited examination within the Contextual Integrity Privacy Theory and Privacy Paradox framework.

The privacy paradox describes the psychological phenomenon where individuals share personal information online, even while acknowledging privacy risks associated with such actions (Brown, 2001; Barth & de Jong, 2017; Bandara et al., 2017). This paradox highlights a disconnect between users' privacy concerns and actual behaviors (Taddicken, 2014). Many users express privacy concerns but still engage in compromise behaviors (Valkenburg & Peter, 2009). Users, particularly youth, often engage in what appears to be contradictory behavior, knowingly exposing private information while recognizing the risks, such as potential misuse by platforms, advertisers, or malicious actors (Hirschprung, 2023).

Various factors contribute to this situation. Many users, particularly youth, lack a complete understanding of the privacy implications, leading them to underestimate the dangers of sharing personal information. In addition, the desire for social validation and awareness often pushes these users to prioritize immediate rewards (like "likes" and "comments") over privacy risks (Trepte & Reinecke, 2011). Peer pressure also plays a significant role, as youth mimic their friends' sharing behaviors

to stay connected and relevant. Despite their concerns, many believe they have control over the information they share. However, sites like TikTok can unexpectedly broaden the reach of content through features like the "For You Page (FYP)," exposing posts to wider audiences than intended (TikTok, 2020).

Youth, who form a crucial demographic for social networking sites, are particularly vulnerable to this privacy paradox. The UN generally defines this age group as those between 15 and 24 (United Nations, 2013), and it is at a formative stage of identity development and social exploration (Islami, 2023). The desire for self-presentation, peer influence, and the lure of instant gratification often overshadow privacy considerations. While many youth feel safe on social networking sites, they frequently worry about how their data might be used and its permanence (Livingstine, 2019). How TikTok amplifies content can further complicate matters, making personal posts visible to unintended audiences.

We can draw from Nissenbaum's *Contextual Integrity Privacy Theory* to better understand these behaviors. This framework emphasizes that sharing information should align with the norms of the context in which it has been shared, shifting our focus from just individual control to the broader socio-technical systems at play. The theory (Nissenbaum, 2009) identifies four key elements: the actors involved (subject, sender, and receiver), the attribute of information (types and sensitivity of shared information), information flows, and transmission principle (the rules governing its transmission). This approach allows researchers to analyze privacy risks through the lens of socio-technical systems rather than isolating the individual. It helps explain how TikTok's design might breach contextual norms, making users' data vulnerable to exploitation.

This study explores the intricate relationship among digital behaviors, privacy concerns, and the technologies that shape them, explicitly focusing on youth interactions with contextual norms. Recognizing TikTok's dual nature, a space for self-expression and a catalyst for data commodification. We highlight the urgent need to address privacy dynamics. Gaining insight into the interactions is essential for devising effective strategies and policies that protect vulnerable users, ultimately fostering a safer online environment for youth.

METHODOLOGY

The research design for this study is grounded in a postpositivist paradigm. Postpositivism, as outlined by Grigoriev (2019), challenges the positivist pursuit of absolute objectivity, emphasizing the role of social construction and context in shaping knowledge. This paradigm fosters methodological pluralism and acknowledges the influence of researcher and participant interactions (Sun, 2024).

Postpositivist approaches, rooted in analytic philosophy and critical realism, aim to balance subjective perspectives with rigorous empirical inquiry (Wilson & Mayrl, 2024).

This study adopts a qualitative approach to exploring privacy concerns among youth TikTok users through Nissenbaum's Contextual Integrity Privacy Theory. It chooses a case study strategy to provide in-depth insights into complex social phenomena (Jensen, 2023). The research focuses on the youth demographic (ages 15-24) as a revelatory case, given their high engagement with TikTok and vulnerability to privacy risks (Grigoriev, 2019). The case study method enables a detailed examination of participants' experiences, aligning with the interpretive nature of postpositivism.

Informants were purposively selected based on specific criteria: 1) TikTok is a daily social networking site; 2) The age range is between 15 and 24, aligning with global organizations' definitions of youth (Livingstone, 2019; United Nations, 2013); 3) Independently manage the TikTok accounts, ensuring autonomy in privacy-related decisions. Seven informants across regions in Indonesia meeting these criteria were recruited to ensure a diverse representation of youth perspectives. This sample size balances depth with breadth in understanding patterns and individual variations. Data were collected through in-depth interviews, a method well-suited for exploring subjective experiences and contextual norms. Semi-structured interviews allowed flexibility to probe deeper into participants' privacy practices while maintaining consistency across core themes. Key areas of inquiry included:

Research conducted data analysis using pattern matching, a robust technique for case studies that enhances internal validity (Yin, 2018). The analysis sought to identify whether participants' privacy practices adhered to or deviated from expected integrity norms. The study also explored the privacy paradox, where individuals knowingly compromise privacy for social validation, a phenomenon prevalent among social media users (Jensen, 2023). Thematic analysis was employed to categorize recurring patterns and exceptions in participants' narratives.

Nissenbaum's Contextual Integrity Privacy Theory provides the conceptual foundation for this study, examining the alignment of data practices with contextual norms. This framework complements postpositivist principles by integrating normative considerations with empirical observations (Sun, 2024). This research provides nuanced insights into youth privacy on TikTok by employing a postpositivist paradigm and qualitative case study design. Combining in-depth interviews, pattern matching, and theoretical grounding in Contextual Integrity

contributes to a comprehensive understanding of privacy management in a digital context. This approach deepens theoretical discourse and offers practical implications for enhancing digital safety for youth.

RESULTS AND DISCUSSION

Seven TikTok users aged between 15 and 24 years were the research participants. Each was selected for its active engagement with TikTok and independent management of their accounts without parental oversight account sharing. These participants' diverse experiences and varying engagement levels provide a nuanced foundation for exploring privacy practices among youth on TikTok. These varied experiences highlight youth users' challenges and opportunities to navigate social networking sites. To protect the identities of the research participants, initials have been used throughout this study.

J, a 15-year-old male, has been using TikTok since 2021. He manages a private account and uses the platform to gain followers, likes, and comments. While J enjoys exploring trending content, he is careful about privacy and avoids posting personal information. Similarly, Ri, a 17-year-old female, also started using TikTok in 2021 but maintains a public account. For Ri, TikTok is a creative outlet where she documents daily activities and expresses herself through relatable and entertaining content. M, a 15-year-old female, began her TikTok journey in 2019 and operates a private account. Unlike Ri, M engages with TikTok sporadically, mainly for entertainment. She values her privacy highly, ensuring her content is accessible only to close friends. In contrast, H, a 16-year-old female who joined TikTok in 2022, actively shares personal experiences and engages with niche communities using her public account. H appreciates TikTok as a source of entertainment and a site to connect with others over shared interests like outdoor activities and sports. N, another 16-year-old female, also started using TikTok in 2022 and maintains a public account. She frequently posts content about her daily life, actively interacting with her audience and seeking validation through likes and comments. RT, a 17-year-old female, has been on TikTok since 2019. She actively participates in prevalent challenges and trends, seeking to grow her audience and increase her visibility on the platform. Similarly, A, a 16-year-old female who joined TikTok in 2019, combines her interest in trending challenges with a desire to monetize her activity on TikTok. A uses a private account but actively balances personal moments with engaging content.

Analyzing participants' responses aged 15-24 revealed a complex understanding of privacy practices shaped by contextual and site-specific factors. Grounded in Helen Nissenbaum's Contextual Integrity Privacy Theory, the results highlighted how

youth navigate privacy concerns by aligning their data practices with contextual expectations of TikTok as a public, algorithm-driven site.

Privacy Practices and Motivations

Participants demonstrated a heightened awareness of privacy risks, which informed their selective sharing practices. Most participants avoided using real names, personal photos, or sensitive information, opting for pseudonyms and generic content. This strategic curation suggests that youth actively engage in privacy management to mitigate the perceived risks of TikTok's wide-reaching audience.

A consistent pattern was the avoidance of using real names or personal photos. As one participant, J, explained, "I use a different name and avoid my real photo because it feels more private this way." Participant Ri echoed this sentiment: "I prefer initials or nicknames. It is not common for people my age to use real names on TikTok."

For many, the motivation behind these practices was rooted in previous exposure to online risks. J recounted, "A friend of mine who did not privatize her account was once DM'd by strangers asking for inappropriate photos. That scared me." Such experiences instilled a strong sense of caution, driving youth to curate their digital identities actively.

The findings revealed their motivations were primarily self-driven and influenced by prior exposure to privacy breaches, online scams, or inappropriate interactions. This explanation reflects a strong internalized sense of agency in managing digital identity, further shaped by cultural norms, including modesty and appropriateness.

Enhance Privacy Practices on TikTok

The study also identified site-specific privacy concerns, emphasizing TikTok's unique challenges compared to other social media. Unlike social networking sites like Instagram or X, TikTok's algorithm and public-facing design were perceived as less secure, leading to frequent utilization of privacy tools, such as account privatization, blocking, and content reporting. Participants frequently utilized TikTok's privacy tools to manage their online presence. H shared, "I block accounts that send me weird DMs. It is my way of staying safe." M reported similar practices, adding, "If i see inappropriate content, i report it immediately. It feels like taking control."

"On TikTok, anyone can see your posts," Ri noted, "so i rarely share anything too personal." This contrasts with their use of Instagram Stories, where familiarity with the audience allows for more openness or even WhatsApp Status. "On WhatsApp, it is just people i know," explained Ri. "So i can share daily life updates." Participants' choices reflect a deliberate approach to privacy, shaped by TikTok's algorithmic design and the perceived risks of exposure. For example, N emphasized, "TikTok's algorithm can make random videos viral, which is why i am cautious about what i share." A mentioned, "On Instagram, I will post personal moments only to my close friends list. On TikTok, i keep it neutral, no personal details."

The study highlighted a unique adaptability in how participants navigate privacy across contexts. Using Nissenbaum's framework, the study revealed how youth align their behaviors with contextual privacy norms. Offline interactions were described as safer due to familiarity. Ri explained, "In person, i know who i am talking to so i am more open. Online, especially on TikTok, i am more guarded." Such adaptability aligns with Nissenbaum's theory (2009), underscoring the importance of context in defining privacy norms and inherently tied to context, such as who the audience is and what platform is.

Despite understanding privacy risks, participants often exhibited behaviors indicative of the privacy paradox. H admitted, "I know sharing too much is risky, but sometimes i just want to follow trends and fit in." The tension, however, reflects the influence of social validation on digital behaviors. Peers and cultural norms significantly shaped participant's decisions. M shared, "My friends' comments often make me reconsider my post. If they think something is too revealing, i will delete it." It aligns with the privacy paradox, where the need for social connection often overrides risk awareness.

While TikTok's features empowered users to manage their privacy, participants expressed dissatisfaction with its privacy policies, describing them as opaque and difficult to comprehend. N commented, "I have tried reading the privacy policy, but it is too complicated. I click agree without fully understanding." Many participants were unaware of TikTok's extensive data collection practices, including sharing practices with third parties. Ri reflected, "I did not know TikTok shares data with advertisers. That feels intrusive." This disconnection between policy and practice highlights a systemic gap in user education, site transparency, and the need for more transparent communication and more accessible privacy frameworks on TikTok.

Participants shared specific expectations for TikTok, such as greater clarity around data sharing by providing actionable recommendations for TikTok to enhance user

privacy. In the first aspect, *transparency*, A suggested, "Let us know what data is being shared and with whom." The second aspect, *control*, M advocated, "Give users the ability to choose what data to share." And the last aspect, *education*, H recommended, "Simplify the privacy policy so we can understand it. The suggestion reflects an increasing call for TikTok accountability that resonates with global discussion on ethical data governance and aligns with Nissenbaum's principles of contextual integrity, emphasizing the importance of aligning privacy practices with users' expectations.

CONCLUSION

In conclusion, this study illustrated a digital privacy reality where 'Now You See Me' highlights the dynamic between digital behaviors, contextual norms, and privacy concerns among youth aged 15-24. This study uses Helen Nissenbaum's Contextual Integrity Privacy Theory as a guiding framework to explore how youth perceive and manage privacy on TikTok. Participants demonstrated an acute awareness of privacy risks, employing strategies such as selective sharing, pseudonym use, and engagement with TikTok's privacy tools. However, their actions also reflected the privacy paradox, wherein the desire for social validation often overshadowed privacy considerations. For instance, participants' willingness to engage with viral content or public challenges frequently conflicted with their efforts to safeguard personal data.

The study emphasizes TikTok's dual role as a medium for creative expression and a source of privacy vulnerabilities. Participants expressed dissatisfaction with the platform's privacy policies and lack of user-friendly educational resources. Recommendations provided by participants include increasing transparency in data-sharing practices, enhancing user control over personal information, and simplifying privacy policies to improve accessibility and comprehension. These findings align with Nissenbaum's principles, emphasizing the necessity of aligning privacy practices with the contextual norms of data sharing. In addition, the research reveals the adaptability of youth in managing privacy across different platforms. Offline interactions were safer due to the familiarity and trust inherent in face-to-face exchanges, whereas online behaviors required stricter self-regulation. Participants' ability to navigate these contextual shifts highlights their resilience and digital literacy despite the challenges posed by TikTok's algorithmic amplification and public-facing design.

While this study offers valuable insights, it is not without limitations. The qualitative design and small sample size, comprising seven participants, limit the generalizability of the findings. Moreover, the focus on Indonesian youth may not

fully capture privacy practices across diverse cultural or regional contexts. Future research should expand the participant pool and employ mixed-method approaches, including surveys and experimental designs, to further explore youth privacy behaviors on TikTok and other social networking sites. Comparative analysis across platforms or demographic groups could yield a broader understanding of privacy management in the digital age.

Ultimately, this study contributes to the theoretical discourse on privacy by applying Contextual Integrity to youth's digital practices. It also provides actionable recommendations for practitioners and policymakers, advocating for the development of safer, more transparent, and inclusive digital environments tailored to the unique needs of youth. By addressing these concerns, platforms like TikTok can foster a healthier balance between creative expression and privacy protection, empowering young users to navigate the digital landscape confidently and securely.

REFERENCES

Adorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite 'nothing to hide' online. *Canadian Review of Sociology*, *56*(1), 8-29. https://doi.org/10.1111/cars.12227

Al Haidar, F., & Tutiasri, R. P. (2023). Strategi Pengelolaan Privasi Remaja pada Orang Tua di Instagram. *Jurnal Ilmu Komunikasi UHO: Jurnal Penelitian Kajian Ilmu Sosial dan Informasi, 8*(3), 510-522. http://dx.doi.org/10.52423/jikuho.v8i3.87

Badillo-Urquiola, K., Page, X., & Wisniewski, P. (2018). Examining Contextual Integrity within Human-Computer Interaction. *Proceedings of the ACM on Human-Computer Interaction, 2(*CSCW), Article 99. https://doi.org/10.1145/3274368

Balleys, C., & Coll, S. (2017). Being publicly intimate: Teenagers managing online privacy. *Media, Culture & Society, 39*(6), 885-901. https://doi.org/10.1177/0163443716679033

Bandara, R., Fernando, M. & Akter, S. (2017). The Privacy Paradox in The Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance. *Procedia Computer Science*. 121: 562-567.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Boyd, D. (2014). *It's Complicated: The Social Lives of Networked Teens*. Yale University Press.

Brown, B. (2001). Studying the Internet Experience. *Hewlett-Packard Company*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=563a300a287ff45eb897d100f26d59d4d87c62c2

Coetzee, G. K. (2017). *Mapping sexuality: Understanding the knowledge, attitudes ,and perceptions of adolescent females towards sexuality and sexual and reproductive health in KwaZulu-Natal, South Africa*. https://core.ac.uk/download/196551410.pdf

De Wolf, R. (2016). Group Privacy Management Strategies and Challenges in Facebook: A Focus Group Study among Flemish Youth Organizations. *Cyberpsychology: Journal of Psychological Research on Cyberspace*, *10*(1). https://doi.org/10.5817/CP2016-1-5

Dwyer, N. (2011). *Traces of Digital Trust: An Interactive Design Perspective* [Doctoral Dissertation, Victoria University]. VU Research Repository.

EDPB. (2021, July 22). Dutch DPA: TikTok Fined for Violating Children's Privacy. *European Data Protection Board*. Retrieved from https://www-edpb-europa-eu.translate.goog/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=sge#:~:text=DPA%20Belanda:%20TikTok%20didenda%20karena%20melanggar%20privasi%20anak%2Danak,-22%20Juli%202021&text=Otoritas%20Perlindungan%20Data%20Belanda%20(DPA,berdasarkan%20undang%2Dundang%20perlindungan%20data

Fiesler, C., & Proferes, N. (2018). Participant perceptions of Twitter research ethics. *Social Media + Society, 4*(1), 1-14. doi:10.1177/2056305118763366

Grigoriev, S. (2019). Postpositivism and The Logic of The Avant-Garde. *History and Theory*, *58*(1): 89-111. https://doi.org/10.1111/hith.12101

Grodzinsky, F., & Tavani, H. T. (2011). Privacy in "The Cloud": Applying Nissenbaum's Theory of Contextual Integrity. *ACM SIGCAS Computers and Society, 41*(1), 38-47. https://doi.org/10.1145/2040787.2040794

Hadi, A. (2023, August 30). Cybersecurity Threats Decreasing, with AI Deployed by Both Sides. *The Jakarta Post*. https://www.thejakartapost.com/business/2023/08/30/cybersecurity-threats-decreasing-with-ai-deployed-by-both-sides.html

Han, S. (2011). Book Review of Helen Nissenbaum Privacy in Context: Technology, Policy, and The Integrity of Social Life. *Journal of Information Policy*. 1:149-151. https://doi.org/10.5325/jinfopoli.1.2011.0149

Hirschprung, R.S. (2023). Is the Privacy Paradox a Domain-Specific Phenomenon *Computers*. 12(8). https://doi.org/10.3390/computers12080156.

Islami, Z. (2023). *Cetak Biru Cinta: Keluarga, Pengabaian, dan Relasi Romantis Idaman*. Akhir Pekan

Jensen, M.J. (2023). Increasing Self-Efficacy and Engagement in Occupational Therapy Education through the Use of an Unfolding Case Study Curricular Design. *Journal of Occupational Therapy Education*. 7(1). https://doi.org/10.26681/jote.2023.070109

Kumar, P. C., Zimmer, M., & Vitak, J. (2024). A Roadmap for Applying the Contextual Integrity Framework in Qualitative Privacy Research. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW1), Article 219. https://doi.org/10.1145/3653710

Kusumastuti, F., Astuti, S.I. & Kurnia, N. (2021). Pengantar Modul Etis Bermedia Digital. In F. Kusumastuti & S.I. Astuti. (Eds.), *Modul Etis Bermedia Digital* (pp. 13-30). Kementerian Komunikasi dan Informatika.

Kuss, D.J. & Griffiths, M.D. (2017). Social Networking Sites and Addiction: Ten Lessons Learned. *International Journal of Environment. Research & Public Health.* 14(3):311. https://doi.org/10.3390/ijerph14030311

Li, H., Yu. L. & Wu, H. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*. *22*(1): 1-6. doi:10.1080/1097198X.2019.1569186

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. An evidence review*. London School of Economics and Political Science. Retrieved from https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

Madden, M., Lenhart, A., Cortesi, S., & Gasser, U. (2013). *Teens, Social Media, and Privacy*. Pew Research Center.

Malkin, N. (2022). Contextual Integrity, Explained: A More Usable Privacy Definition. *IEEE Security & Privacy, 20*(6), 16-25. https://doi.org/10.1109/MSEC.2022.3201585

Marwick, A., Fontaine, C., & Boyd, d. (2017). Nobody Sees It, Nobody Gets Mad: Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. *Social Media + Society, 3*(2). https://doi.org/10.1177/2056305117710455

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and The Integrity of Social Life*. Stanford University Press.

Rinestu, Y., & Handayani, W. (2021). Manajemen privasi komunikasi media sosial Twitter oleh mahasiswa UNY. *Jurnal Komunikasi dan Sosial, 2*(1), 22-32. https://doi.org/10.12345/jks.v2i1.41668

Riyanto, GP & Pratomo, Y. (2023, September 19). TikTok Didenda Rp 5,6 Triliun, Buntut Kasus Pelanggaran Privasi Anak. *Kompas.com*. https://tekno.kompas.com/read/2023/09/19/13050017/tiktok-didenda-rp-56-triliun-buntut-kasus-pelanggaran-privasi-anak?page=all

Roderick, M. (2020, September 2). The Average Social Media Privacy Policy Takes an Hour to Read. *The Realtime Report. Retrieved from* https://therealtimereport.com/2020/09/02/the-average-social-media-privacy-policy-takes-an-hour-to-read/

Saraswati, I. (2021). Melihat peran perantara dalam kasus penyebaran video non-konsensual dengan kerangka contextual integrity. *Jurnal Wanita dan Keluarga, 2*(2), 93-106. https://doi.org/10.22146/jwk.3618.

Siibak, A. & Traks, K. (2019). The Dark Sides of Sharenting. *Catalan Journal of Communication and Cultural Studies*, *11*(1): 115-121. DOI: https://doi.org/10.1386/cjcs.11.1.115_1

Smirnova, Y. & Morales, V.T. (2024). Understanding Challenges of GDPR Implementation in Business Enterprises: A Systematic Literature Review. *International Journal of Law and Management*. DOI:10.1108/IJLMA-08-2023-0170

Sun, Y. (2024). Emerging Dialogue on Postpositivist Philosophies of the Social Sciences. *Innovation in the Social Sciences, 2*(2): 119-122

Taddicken, M. (2014). The Privacy Paradox in The Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self Disclosure. *Journal of Computer-Mediated Communication*, *19*(2): 248-273. https://doi.org/10.1111/jcc4.12052

Thompson, J. (2011). Communication privacy management in college athletics: Exploring privacy dilemmas in the athletic/academic advisor student-athlete interpersonal relationship. *Journal of Applied Sport Management, 3*(1), 44-60. https://trace.tennessee.edu/jasm/vol3/iss1/14

TikTok. (2020, June 19). Bagaimana TikTok Rekomendasikan Video #ForYou. *TikTok*. https://newsroom.tiktok.com/in-id/for-you-page

Trepte, S., & Reinecke, L. (Eds.). (2011). *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer-Verlag Berlin Heidelberg. https://doi.org/10.1007/978-3-642-21521-6

Trninic, D., & Kupresanin Vukelic, A. (2021). Privacy on the Internet Concerning Generation Z in Bosnia and Herzegovina. *Media Literacy and Academic Research, 4*(1), 180-196. https://doi.org/10.12345/mlar.2021.01

United Nations. (2013). *Definition of Youth*. UN Youth. https://www.un.org/esa/socdev/documents/youth/fact-sheets/youth-definition.pdf

Valkenburg, P. M., & Peter, J. (2009). Social consequences of the Internet for adolescents: A decade of research. *Current Directions in Psychological Science, 18*(1), 1-5. https://doi.org/10.1111/j.1467-8721.2009.01595.x

Kemp, S. (2024, January). Digital 2024: 5 Billion Social Media Users. *We Are Social*. https://wearesocial.com/id/blog/2024/01/digital-2024-5-billion-social-media-users/

Wilson, N.H. & Mayrl, D. (2024). *After Positivism: New Approaches to Comparison in Historical Sociology*. Columbia University Press.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods (6th ed.).* SAGE Publications Inc.

Zhang, R., & Fu, J. S. (2020). Privacy Management and Self-Disclosure on Social Network Sites: The Moderating Effects of Stress and Gender. *Journal of Computer-Mediated Communication, 25*(3), 236-251. https://doi.org/10.1093/jcmc/zmaa004