

ALTER ACCOUNTS AS SAFE SPACES IN GENERATION Z PRIVACY MANAGEMENT ON INSTAGRAM

Mika Lorensia Ginting

UPN “Veteran” Jawa Timur
mikalorensia@gmail.com

Roziana Febrianita

UPN “Veteran” Jawa Timur
Corresponding author email: roziana.ilkom@upnjatim.ac.id

Abstract

Social media's rapid growth has transformed how Generation Z builds relationships, constructs identities, and manages privacy online. On Instagram, the use of both main and alter accounts reflects a shift in privacy management, where users regulate access to personal information through interaction restriction features based on audience, context, and perceived risk. Despite widespread use of these practices, little research has examined how such features shape Generation Z's privacy management. This study therefore examines how Generation Z manages privacy through Instagram's interaction restriction features on main and alter accounts, using a descriptive qualitative approach within a constructivist paradigm. Data were collected through in-depth interviews, observation, and documentation involving ten Generation Z participants aged 18–25 who actively use both account types and have experience with these features. Data were analyzed using Communication Privacy Management (CPM) theory, focusing on privacy boundaries, privacy rules, and boundary turbulence. Findings show that privacy management is dynamic, layered, and relational: boundaries are formed by separating main and alter account functions and using features like Private Account, Close Friends, Hide Story, Mute, and Block; rules are shaped by relational closeness, gender, context, and risk perception; and turbulence arises when private information reaches unintended audiences or restrictions strain relationships.

Keywords: Generation Z; privacy management; Instagram alter account; interaction restriction features; Communication Privacy Management theory

INTRODUCTION

The development of digital communication technology has transformed the way individuals build social relationships, share information, and present themselves to others. Social media is no longer used merely as a communication tool, but has also become a social space where users construct identities, maintain relationships, express emotions, and negotiate boundaries between private and public life. One of the social media platforms widely used in this process is Instagram. Through features such as photo and video posts, Stories, Reels, Direct Messages, comments, and various privacy settings, Instagram allows users to share everyday activities while also managing how their information can be accessed by others.

In the context of Generation Z, Instagram occupies an important position because this generation has grown up alongside the development of digital technology and is highly familiar with the use of social media in daily life. Generation Z does not only use Instagram to communicate, but also to build self-image, express personal experiences, document everyday moments, and maintain relationships with different social groups. However, the practice of sharing information on Instagram is not free from privacy risks. Every post, Story, or interaction can be seen, judged, saved, commented on, or redistributed by certain audiences. This condition requires users to consider the extent to which personal information should be disclosed in digital spaces.

Privacy issues on Instagram become more complex because one account can bring together various types of audiences in the same digital space. In a single account, users may be connected with close friends, family members, school friends, university friends, organizational networks, lecturers, coworkers, and newly known acquaintances. These different audiences may have different expectations regarding how users should present themselves. Content that is considered acceptable by peers may not be interpreted in the same way by family members or more formal relations. This situation creates the possibility of context collapse, where different social contexts meet in one digital space. As a result, users need to manage the information they share and determine which audiences are allowed to access particular aspects of their personal lives.

One strategy commonly used by Generation Z to deal with this condition is the use of more than one Instagram account, namely a main account and an alter account. The main account is generally used to present a more organized, controlled, and socially acceptable self-image to a wider audience. On this account, users tend to be more careful in selecting what to post because they consider the possible judgments of different audience groups. In contrast, the alter account functions as a more personal and limited space. Through alter accounts, users feel more comfortable sharing daily activities, emotional expressions, spontaneous posts, memories with close friends, or content that they consider unsuitable for their main account.

Although alter accounts are often perceived as safer and more private spaces, their existence does not completely eliminate privacy risks. Information shared on alter accounts can still move beyond the intended boundaries when audiences take screenshots, record screens, tell others about the content, or redistribute posts through certain platform features. In addition, alter accounts can also be discovered by unintended audiences through account recommendations or network connections within Instagram. Therefore, alter accounts cannot be understood as fully closed private spaces. Instead, they should be seen as digital spaces that still require active and continuous privacy management.

The management of privacy in the use of main and alter Instagram accounts can be understood through Sandra Petronio's Communication Privacy Management Theory. This theory explains that individuals have ownership of their private information and have the right to determine how that information is shared with others. Privacy is not understood as a completely closed condition, but as a process of managing the boundary between information that is kept private and information that is disclosed. Individuals create privacy boundaries to determine who may know certain information, establish privacy rules to regulate how information may be shared, and face possible boundary disruptions when the rules they have created do not work as expected.

Communication Privacy Management consists of three main concepts that are relevant to this study: privacy boundaries, privacy rules, and boundary turbulence. Privacy boundaries refer to the lines individuals create to distinguish between private information and information that may be shared with particular audiences. In the context of Instagram, these boundaries can be seen through the separation between main and alter accounts, the use of private account settings, the Close Friends feature, and the practice of hiding Stories from certain people. Privacy rules refer to the considerations used by individuals in deciding to whom, when, and to what extent private information may be disclosed. These rules may be shaped by relational closeness, trust, type of content, gender of the audience, family norms, situational context, and perceived risks. Meanwhile, boundary turbulence refers to disruptions that occur when privacy boundaries do not function as expected, such as when information is shared without permission or when unintended audiences gain access to certain content.

In addition to separating their accounts, Generation Z users also utilize various interaction restriction features provided by Instagram to manage privacy. The Private Account feature allows users to filter who can follow them and view their posts. Close Friends enables users to share Stories only with selected people who are considered closer or more trustworthy. Hide Story allows users to prevent certain individuals from seeing specific content without directly cutting off the relationship. Mute is used to reduce exposure to someone's content without unfollowing them. Remove Followers and Block are used to revoke access when someone is no longer considered safe, close,

or comfortable to keep within the user's digital space. Furthermore, settings related to comments, Story replies, and resharing can also be used to limit how audiences respond to shared content.

The use of these features shows that privacy on Instagram is not merely about deciding whether or not to share information. It also involves managing audiences, limiting responses, and adjusting digital connections. In practice, users may allow someone to access their content in one situation but restrict the same person in another. This indicates that privacy management is dynamic and contextual. Privacy boundaries are not fixed; they may change depending on experience, social relationships, emotional comfort, and perceived risk.

The main problem addressed in this study is how Generation Z manages privacy through interaction restriction features on main and alter Instagram accounts. This issue is important because alter accounts are often viewed as spaces for freer self-expression, yet they still contain privacy risks. Users may feel more comfortable sharing information on alter accounts because the audience is more limited, but a limited audience does not always guarantee that information will remain within the intended space. Therefore, it is necessary to understand how users form boundaries, create privacy rules, and deal with privacy disruptions in their use of main and alter accounts.

Previous studies on privacy management on Instagram have often focused on specific features, such as Close Friends or private accounts, or on the relationship between second accounts and self-disclosure. However, studies that specifically examine the relationship between main accounts, alter accounts, and various interaction restriction features as an integrated practice of privacy management still need further development. In users' actual experiences, privacy management is not carried out through a single feature, but through a combination of platform features and social considerations. Users may set their account to private, use Close Friends, hide Stories, mute accounts, remove followers, or block someone depending on the situation they face. Therefore, this study seeks to examine privacy management more comprehensively in the context of Instagram use among Generation Z.

Based on the explanation above, this study aims to analyze how Generation Z manages privacy through the use of interaction restriction features on main and alter Instagram accounts. This study is expected to contribute theoretically to the development of Communication Privacy Management studies in the context of digital communication, particularly in understanding how social media users construct layered and dynamic privacy boundaries. Practically, this study is also expected to provide insight for Instagram users regarding the importance of managing access, responses, and the risks of personal information circulation in digital spaces.

RESEARCH METHOD

This study uses a descriptive qualitative approach to understand how Generation Z manages privacy through interaction restriction features on main and alter Instagram accounts. A qualitative approach is considered appropriate because this research does not aim to measure privacy management statistically, but to explore the meanings, experiences, considerations, and social practices behind users' decisions in managing access to personal information. Through this approach, the researcher seeks to describe how individuals interpret privacy, determine audiences, use Instagram features, and respond to privacy disruptions in their digital interactions. The descriptive nature of this research allows the findings to be presented in a detailed and systematic way based on the experiences of the informants.

The data collection process was carried out through in-depth interviews, observation, and documentation. In-depth interviews were used as the main technique because they allowed the researcher to obtain detailed explanations from informants regarding their experiences in using Instagram, particularly in managing main and alter accounts. The interviews were conducted in a semi-structured manner, meaning that the researcher prepared several guiding questions but still allowed flexibility for informants to explain their experiences freely. The interview questions focused on the reasons for using more than one Instagram account, differences between main and alter accounts, criteria for accepting followers, the use of interaction restriction features, and experiences related to privacy disturbances. This technique enabled the researcher to explore not only what informants did, but also why they made certain privacy-related decisions.

Observation was used as a supporting technique to strengthen the interview data. In this study, observation was conducted by examining the visible practices of privacy management on informants' Instagram accounts, such as the use of private accounts, Close Friends, Hide Story, Mute, Remove Followers, Block, and other interaction settings. The observation did not aim to interfere with the informants' activities, but to understand how privacy management was practiced in a real digital context. Documentation was also used as complementary data, including screenshots or other relevant materials related to the use of Instagram privacy features. All documentation was collected with the consent of the informants and handled carefully to protect their privacy and identity.

The data sources in this study consisted of primary and secondary sources. The primary data were obtained directly from ten Generation Z informants who met the research criteria. The informants were individuals aged approximately 18 to 25 years old, actively used Instagram, had both a main account and an alter account, and had experience using interaction restriction features to manage privacy. The selection of informants was conducted purposively, meaning that participants were chosen based on their relevance to the research focus. This selection was important because the study

required informants who had direct experience in managing privacy through multiple Instagram accounts and platform features. Secondary data were obtained from books, journal articles, previous research, and other academic references related to Generation Z, Instagram, alter accounts, privacy management, self-disclosure, and Communication Privacy Management Theory.

The types of data used in this research were qualitative data in the form of verbal explanations, narratives, observations, and documentation. The interview data consisted of informants' statements about their experiences, perceptions, and considerations in using Instagram features to regulate privacy. Observation data included descriptions of how informants separated audiences and managed access through different accounts or features. Documentation data served as supporting evidence to complement the interview and observation results. These data were not numerical, but interpretive, because they reflected the meanings and social contexts behind the informants' privacy management practices.

Data analysis was conducted using the interactive model of Miles and Huberman, which includes data reduction, data display, and conclusion drawing. In the data reduction stage, the researcher selected and organized information that was relevant to the focus of the study, such as the use of main and alter accounts, privacy boundaries, privacy rules, and privacy disturbances. Irrelevant or repetitive data were simplified, while important statements were grouped into specific themes. In the data display stage, the reduced data were arranged in the form of descriptive narratives and thematic categories to make patterns easier to identify. The data were then interpreted using Communication Privacy Management Theory, particularly the concepts of privacy boundaries, privacy rules, and boundary turbulence. Finally, conclusions were drawn by comparing the patterns found across informants and relating them to the research problem. Through this process, the study was able to explain how Generation Z manages privacy on Instagram as a layered, dynamic, and relational practice.

RESULT AND DISCUSSION

The findings of this study show that Generation Z manages privacy on Instagram through layered, dynamic, and relational practices. Based on in-depth interviews with ten informants, supported by observation and documentation, privacy management is not only carried out by separating main and alter accounts, but also by using interaction restriction features provided by Instagram. The informants in this study have two to four Instagram accounts, with different functions, audiences, and levels of openness. The main account is generally used to present a more organized and controlled self-image, while the alter account is used as a more personal space to share daily activities, emotional expressions, spontaneous moments, and content that is considered unsuitable for wider audiences.

The findings are discussed using Communication Privacy Management Theory, especially through three main concepts: privacy boundaries, privacy rules, and boundary turbulence. These concepts help explain how informants create boundaries, determine rules for sharing information, and respond to privacy disruptions that occur in their digital interactions.

Privacy Boundaries in Main and Alter Instagram Accounts

The first finding shows that informants create privacy boundaries by separating the functions of their main and alter accounts. This separation becomes the first layer of privacy management. The main account is usually directed toward a wider and more diverse audience, such as university friends, acquaintances, organizational relations, family members, and other people who are not necessarily close to the informant. Because of this wider audience, informants tend to be more careful in choosing what to upload on their main accounts.

Several informants stated that their main accounts are used to upload content that looks neat, proper, aesthetic, or socially acceptable. For example, one informant explained that the main account is used for “good photos,” formal activities, and moments that are suitable to be seen by many people. Another informant described the main account as a space to show a more positive and organized version of the self. This shows that the main account functions as a public-facing space where users manage their self-image more carefully.

In contrast, alter accounts are used as more personal spaces. Informants use alter accounts to share daily activities, random posts, personal stories, emotional expressions, complaints, memories with close friends, and content that they would not upload on their main accounts. One informant stated that the alter account is a space where they can be more spontaneous and “upload anything” without thinking too much about aesthetics. Another informant explained that the alter account is used to share daily life and personal moments because the main account feels too formal and too visible to wider audiences.

However, the alter account is not automatically a fully private or risk-free space. Even though the audience is more limited, informants still consider who can access the account and how the content may be interpreted. This means that the alter account becomes a more private space compared to the main account, but it still requires active privacy management.

Observation also supports this finding. The use of alter accounts shows a clear distinction between public self-presentation and personal expression. Main accounts tend to contain more selected and polished content, while alter accounts are more flexible and informal. This reflects the idea that Generation Z does not treat Instagram as one uniform space. Instead, they divide their digital interactions into different spaces based on audience, content, and level of personal disclosure.

Use of Instagram Features as Privacy Boundaries

The second finding shows that informants use Instagram's interaction restriction features as technical tools to strengthen their privacy boundaries. These features include Private Account, Close Friends, Hide Story, Mute, Remove Followers, Block, and Unfollow. These features are not used randomly, but based on the informants' needs to regulate access, interaction, and visibility.

Private Account becomes the most basic boundary used by informants, especially on alter accounts. Most informants set their alter accounts to private so they can filter who is allowed to follow and view their content. This feature allows users to control access from the beginning, before any information is shared. One informant explained that a private account helps them "filter who enters" the account. Another informant stated that Instagram contains their "inner side," so not everyone should be allowed to see it.

This shows that Private Account is not only a technical feature, but also a symbolic boundary. It allows informants to decide who may enter their personal digital space. In Communication Privacy Management Theory, this practice reflects privacy boundary formation, where individuals create limits between private information and public access.

Close Friends is used as an additional layer of privacy. Interestingly, even when the alter account is already private, some informants still use Close Friends to limit certain content to a smaller group. This shows that followers in a private alter account are not always considered equally trustworthy. Informants still make distinctions between ordinary followers and people who are considered closer, safer, or more trusted.

For example, one informant stated that there are some followers who are still feared because they may judge or misunderstand the content. Another informant said that Close Friends is used because there are certain things they want some people to see, but not others. This indicates that privacy boundaries on Instagram are layered. The private account limits general access, while Close Friends limits access to more sensitive or personal content.

Hide Story is used as a more situational privacy feature. Informants use this feature to hide certain content from specific people without removing or blocking them. This feature is often used when informants still want to maintain a social relationship but do not want particular people to see certain posts. Some informants use Hide Story to hide content from family members, relatives, partners, or friends who may respond negatively.

For instance, one informant stated that they often hide Stories from family members when uploading content related to a romantic relationship. Another informant explained that they hide Stories from close friends when they are afraid of being scolded or judged. This shows that privacy boundaries are not only determined

by closeness. Sometimes, close people can also be restricted because they may give strong emotional responses, advice, or judgment.

Mute is used to manage the presence of others in the informant's digital space. Unlike Hide Story, which controls who can see the informant's content, Mute controls what the informant sees from others. Several informants use Mute when they do not want to see someone's posts or Stories but still want to maintain the relationship. One informant explained that they mute someone because they do not want to see anything that person posts, but still want to maintain a good relationship. Another informant said that some content gives "bad energy," so muting becomes a way to protect emotional comfort.

Remove Followers, Block, and Unfollow are used when the informants feel the need to reduce or revoke access. Remove Followers is used when someone is no longer considered close, when there is no interaction, or when the person becomes a silent viewer. One informant removed followers because they felt those people were no longer close or never interacted. Another informant removed someone because the person was known to talk about them behind their back.

Block is used in more serious situations, such as when dealing with fake accounts, spam, stalkers, former close relations, or people who create discomfort. One informant blocked fake accounts because they were considered disturbing and too curious about the informant's life. Another informant blocked a former close friend because of conflict. These findings show that blocking is used as a stronger form of boundary termination when softer restrictions are no longer enough.

Privacy Rules in Managing Audiences and Content

The third finding shows that informants apply certain privacy rules when deciding who can access their accounts or specific content. These rules are not always written or explicitly stated, but they appear consistently in the informants' decisions. Based on the interview data, five main criteria shape the privacy rules of Generation Z in this study: relational closeness, gender, situational context, family and environmental norms, and risk consideration.

The most dominant criterion is relational closeness. Informants generally allow wider audiences to access their main accounts, but only closer and more trusted people can access their alter accounts. One informant explained that people who have only met them casually may be accepted into the main account, but only close and trusted people are accepted into the alter account. Another informant stated that the alter account is only for people who are involved in their everyday life.

This finding shows that access to alter accounts is treated as a form of trust. Being accepted into an alter account means that the person is considered safe enough to see a more personal side of the informant. In the framework of Communication Privacy Management Theory, this reflects the way individuals create rules for who may become co-owners of their private information.

Gender also becomes an important criterion for some informants. Several female informants limit certain content only to female friends, especially content related to self-photos, personal feelings, or more sensitive expressions. One informant stated that although their alter account includes both male and female followers, the Close Friends list only contains close female friends. Another informant explained that they were cautious because even a female friend's account might be accessed by their male partner. This shows that privacy rules are influenced not only by direct trust toward the audience, but also by the possibility that information may be seen by unintended people through that audience.

Situational context also shapes privacy rules. Informants may change their privacy settings depending on the type of content, emotional condition, relationship dynamics, or specific events. Someone who was once considered safe may later be removed, hidden, or excluded from Close Friends if there is conflict or discomfort. One informant stated that one uncomfortable incident can make someone no longer safe to access their personal content. This shows that privacy rules are dynamic and can change over time.

Family and environmental norms also influence privacy management. Some informants restrict family members, relatives, or people connected to family because they fear judgment, monitoring, or being reported to parents or siblings. This finding is important because it shows that biological closeness does not automatically mean access to all personal information. Family members may be emotionally close, but they may also carry norms, expectations, and forms of control that make users more careful.

Risk consideration is another important privacy rule. Even in alter accounts, informants still think about how others might interpret their posts. Some informants are afraid that their followers may feel annoyed, judge them, or misunderstand their posts. Because of this, some content is not uploaded at all and is kept only in the phone gallery. This shows that the strongest form of privacy control is sometimes not sharing information in any digital space.

Boundary Turbulence in Alter Account Use

The fourth finding shows that privacy boundaries do not always work as expected. Even after informants set accounts to private, use Close Friends, or hide Stories, privacy disruptions still occur. In Communication Privacy Management Theory, this condition is called boundary turbulence.

The first form of turbulence found in this study is interpersonal turbulence. This happens when audiences who already have access fail to maintain the expected privacy boundary. Some informants experienced or knew about Stories being screenshotted, screen recorded, reposted, or told to people outside the intended audience. One informant shared that their Story was screenshotted and sent to another person. Another informant experienced a video being screen recorded by one of their followers,

but they did not know who did it. This creates uncertainty and makes the informant more cautious in future posts.

This finding shows that allowing someone to see content does not mean allowing them to save or redistribute it. However, not all audiences understand this boundary in the same way. In CPM terms, once information is shared, the audience becomes a co-owner of that information. Problems arise when the co-owner does not follow the original owner's expected privacy rules.

The second form is platform turbulence. This occurs when Instagram's system or features make information or accounts more visible than intended. For example, repost features may allow content to reach people outside the original audience. Account recommendation features may also cause alter accounts to be discovered by unintended people. One informant stated that their alter account was found by a senior through Instagram suggestions. This shows that privacy management is not only affected by users and audiences, but also by the platform's design.

The third form is detection turbulence. This happens when someone realizes that they have been hidden, removed, or excluded from Close Friends. In this case, the problem is not that content is leaked, but that the act of restricting becomes visible. Some informants were asked why they removed someone or why someone could no longer see certain content. To avoid conflict, informants often gave indirect explanations, such as saying it was accidental or that the content was only edited for certain people.

Overall, informants tend to respond to boundary turbulence in non-confrontational ways. They do not always directly confront the person who violates privacy. Instead, they become more careful, change their Close Friends list, remove followers, hide Stories, reject follow requests, or reduce the amount of personal content shared. This shows that privacy management is a continuous process. Boundaries are not fixed once they are created; they are adjusted based on experience, discomfort, and perceived risk.

ANALYSIS AND DISCUSSION

The findings of this study show that Generation Z manages privacy on Instagram through layered, dynamic, and relational practices. Privacy management is not only carried out by separating main and alter accounts, but also through the use of interaction restriction features such as Private Account, Close Friends, Hide Story, Mute, Remove Followers, Block, and Unfollow. These findings are consistent with Communication Privacy Management Theory, which explains that individuals act as owners of private information and create boundaries to regulate how such information is accessed, shared, and protected.¹ In the context of Instagram, these boundaries are

¹ Sandra Petronio, *Boundaries of Privacy: Dialectics of Disclosure* (Albany: State University of New York Press, 2002)

not only interpersonal but also technological because users rely on platform features to manage the visibility of their personal information.

The first important finding is that the separation between main accounts and alter accounts functions as a macro-level privacy boundary. Most informants use their main accounts as more public and controlled spaces, while alter accounts are used as more personal and selective spaces. The main account is generally used to present a socially acceptable image, such as formal activities, aesthetic photos, organizational activities, or moments considered appropriate for a wider audience. In contrast, alter accounts are used to share spontaneous posts, emotional expressions, daily activities, personal stories, and content that users do not want to display on their main accounts. This finding supports the idea that social media users manage self-disclosure by separating audiences and adjusting the type of information shared in each digital space.²

The use of multiple accounts also shows that Generation Z does not treat Instagram as a single homogeneous communication space. Instead, users divide their digital interactions according to audience, content, and level of intimacy. This practice is related to the phenomenon of Finstagram or fake Instagram, where alternative accounts are used to manage identity and privacy in more selective ways.³ Alter accounts allow users to present a more personal side of themselves while still maintaining control over who can access that side. However, the findings also show that alter accounts do not completely eliminate privacy risks. Even within alter accounts, informants still think about whether their posts may be judged, misunderstood, saved, or spread by others.

The second finding shows that Instagram features function as micro-level privacy boundaries. Private Account is used as the first gate to filter followers before they can access personal content. Close Friends is used as an additional layer of privacy, especially when users want to share more sensitive content with a smaller and more trusted audience. This finding is in line with previous research showing that the Close Friends feature becomes a selective space for self-disclosure and emotional expression among Instagram users.⁴ In this study, Close Friends is not only used on main accounts but also on alter accounts, which shows that even private alter accounts still require further audience filtering.

Hide Story is another important feature used by informants to regulate content visibility. Unlike Close Friends, which selects who can see certain content, Hide Story works by excluding specific people from viewing particular posts. Several informants use Hide Story to limit access from family members, relatives, partners, or friends who

² H. Tandres and S. Winduwati, "Pengelolaan Self-Disclosure Generasi Z Melalui Penggunaan Multiple Accounts di Instagram," *Koneksi* 8, no. 1 (2024): 233–244,

³ C. Desideria and A. R. Syaki, "Fake Instagram: Manajemen Identitas dan Privasi Melalui Fenomena Finstagram," *Tuturlogi* 3, no. 2 (2022),

⁴ F. A. Annabillah and K. M. Boer, "Fitur Close Friends Instagram sebagai Keterbukaan Diri Mahasiswa yang Mengalami Kecemasan Bermedia Sosial," *Jurnal Indonesia: Manajemen Informatika dan Komunikasi* 4, no. 3 (2023): 1550–1565,

may give unwanted responses. This shows that closeness does not always mean full access. A person may be socially close but still be restricted because they are considered likely to judge, question, or monitor the informant's activities. This finding is closely related to previous studies on teenage privacy in social media, which show that young users manage privacy by controlling friendship boundaries and visibility settings.⁵

Mute, Remove Followers, Block, and Unfollow are used to regulate digital presence and access after a relationship has already been formed. Mute is used when informants do not want to see someone's posts or Stories but still want to maintain a social relationship. Remove Followers is used when someone is no longer considered close, trusted, or relevant to remain inside the user's personal digital space. Block is used in more serious situations, such as when users deal with fake accounts, stalkers, spam, conflict, or people who create discomfort. These features show that privacy management is not only about controlling who can see information, but also about managing emotional comfort, social distance, and relational boundaries. This is relevant to the view that Instagram plays an important role in shaping social interaction and digital ethics among Generation Z.⁶

The third finding concerns the privacy rules used by informants when determining who can access their main accounts, alter accounts, and specific content. Based on the interview data, five main criteria shape these privacy rules: relational closeness, gender, situational context, family and environmental norms, and risk consideration. Relational closeness is the most dominant criterion. Informants tend to allow broader audiences to follow their main accounts, but only close friends, trusted people, or those involved in their daily lives are allowed into alter accounts. This finding supports the idea that multiple Instagram accounts are used to manage self-disclosure based on different levels of audience closeness and trust.⁷

Gender also becomes an important criterion, especially among female informants. Some female informants limit specific content, such as personal photos or emotional stories, only to female friends. This shows that privacy rules are shaped not only by closeness but also by the perceived safety of the audience. Female informants may feel more comfortable sharing certain content with women because they consider the possibility of being misunderstood, judged, or seen by unintended male audiences. This finding is consistent with studies on self-disclosure among Generation Z, which show that disclosure practices are influenced by emotional comfort, confidence, and audience perception.⁸

⁵ F. R. Hidayati and Irwansyah, "Privasi 'Pertemanan' Remaja di Media Sosial," *Jurnal Teknologi dan Sistem Informasi Bisnis* 3, no. 1 (2021): 78–91,

⁶ W. Ramadhina et al., "Peranan Media Sosial Instagram terhadap Interaksi Sosial dan Etika pada Generasi Z," *Journal on Education* 6, no. 2 (2024): 11029–11037.

⁷ I. K. C. W. Angga and H. B. Nugroho, "Konstruk Sosial dan Teknologi: Fenomena Penggunaan Fitur Close Friends dalam Second Account Instagram," *Jurnal Riset Komunikasi (Jurkom)* 8, no. 2 (2025): 308–327.

⁸ W. O. D. C. Rahmad, M. Mau, and M. Akbar, "Self-Disclosure Mahasiswa Ilmu Komunikasi di Instagram: Studi Kualitatif tentang Ekspresi Diri di Era Digital," *Jurnal Ilmu Komunikasi (J-IKA)* 12, no. 1 (2025): 9–15.

Situational context also affects privacy rules. Informants may change their Close Friends list, hide specific users, remove followers, or even create new accounts when they experience discomfort or conflict. A person who was once considered safe may later become unsafe when the relationship changes. This shows that privacy rules are not permanent but are constantly revised according to social experience. The dynamic nature of privacy management is also related to the privacy paradox faced by Generation Z, where users want to share personal information but remain concerned about possible risks in digital spaces.⁹

Family and environmental norms are also significant in shaping privacy boundaries. Several informants restrict family members, relatives, or people connected to family because they fear being monitored, judged, or reported. This shows that biological closeness does not automatically mean unrestricted access to personal information. Family members may be close, but they may also represent social norms and control. Therefore, informants use alter accounts or Hide Story to separate peer-based expression from family-based expectations. This finding is also relevant to the idea that social media can shift interaction patterns among young people because users must continuously adjust their communication practices based on the audience they face.¹⁰

Risk consideration becomes the final criterion in privacy rules. Although alter accounts are considered more private, some informants still choose not to upload certain content at all. They keep some photos, videos, or emotional expressions only in their phone gallery because they fear judgment, misunderstanding, or leakage. This shows that the strongest form of privacy management is sometimes non-disclosure. In Communication Privacy Management Theory, once private information is shared, the audience becomes a co-owner of that information.¹¹ Therefore, not uploading certain content becomes a way for informants to keep full ownership over their personal information.

The fourth finding shows that privacy boundaries do not always work as expected. This condition is known as boundary turbulence.¹² In this study, boundary turbulence appears in three forms: interpersonal turbulence, platform turbulence, and detection turbulence. Interpersonal turbulence occurs when audiences who have been given access fail to maintain the expected privacy boundary. Some informants experienced or knew about Stories being screenshotted, screen recorded, reposted, or told to people outside the intended audience. This indicates a mismatch between what the user expects and what the audience does after receiving access to personal information.

⁹ S. Tania, "Mengeksplorasi Paradoks Privasi Gen-Z dalam Personalisasi Iklan di Media Digital," *Interaksi: Jurnal Ilmu Komunikasi* 12, no. 1 (2023): 50–6

¹⁰ I. Putri et al., "Media Sosial sebagai Media Pergeseran Interaksi Sosial Remaja," *Jurnal Ilmu Komunikasi Balayudha* 2, no. 2 (2022): 1–10.

¹¹ Sandra Petronio, *Boundaries of Privacy: Dialectics of Disclosure*.

¹² Sandra Petronio and Ashley Hernandez, "Communication Privacy Management Theory," *Oxford Research Encyclopedia of Communication* (2019)

Platform turbulence occurs when Instagram's system or features make information or accounts more visible than intended. For example, repost features may allow content to move beyond its original audience, while account recommendation features may cause alter accounts to be discovered by unintended people. This shows that privacy management is not only shaped by users and audiences, but also by platform architecture. Although Instagram provides privacy features, it also encourages visibility, connectivity, and content circulation. This finding is relevant to studies showing that digital platforms create both opportunities for expression and risks for privacy management.¹³

Detection turbulence occurs when restriction actions become visible to the restricted person. For instance, someone may realize that they have been removed from followers, excluded from Close Friends, or hidden from seeing certain Stories. In this case, the problem is not necessarily that content is leaked, but that the act of restriction becomes socially visible. Informants often respond by giving indirect explanations to avoid conflict, such as saying that the removal was accidental or that the Story setting was only temporary. This shows that privacy management on Instagram is also relational because restricting someone can be interpreted as rejection, distrust, or social distance.

Overall, these findings show that Generation Z's privacy management on Instagram is a continuous negotiation between self-expression, audience control, emotional comfort, social relationships, and platform risks. Alter accounts provide more freedom than main accounts, but they do not remove the need for privacy control. Instead, alter accounts become spaces where privacy boundaries are repeatedly created, tested, disturbed, and adjusted. This supports the view that second accounts are related to self-disclosure and privacy management among Generation Z.¹⁴ The findings also reflect the broader condition of digital culture in Indonesia, where social media use continues to grow and young users become active participants in online interaction.¹⁵

Thus, privacy management among Generation Z cannot be understood only as the use of technical features. It is also a social and relational process shaped by trust, closeness, gender, family norms, emotional comfort, and perceived risk. Instagram features help users regulate access and interaction, but they cannot fully guarantee privacy. Therefore, Generation Z users must continuously evaluate who is allowed to enter their digital space, what kind of information can be shared, and how to respond when privacy boundaries are disrupted.

¹³ P. W. Aji, P. Utari, and Sudarmo, "Manajemen Privasi Generasi Z dalam Menghadapi Komersialisasi Data Pribadi di Media Sosial," *Jurnal IPTEK-KOM* 24, no. 2 (2022): 103–116.

¹⁴ N. Zahrah, S. Suhasman, and M. Akbar, "Pengaruh Second Account Instagram terhadap Pengungkapan Diri dan Manajemen Privasi Generasi Z," *Al-Kalam: Jurnal Komunikasi, Bisnis dan Manajemen* 12, no. 1 (2025)

¹⁵ We Are Social and Meltwater, *Digital 2025: Indonesia* (2025), <https://wearesocial.com>

CONCLUSION

This study concludes that Generation Z manages privacy on Instagram through a layered, dynamic, and relational process. Privacy management is not only carried out by separating main accounts and alter accounts, but also through the use of interaction restriction features such as Private Account, Close Friends, Hide Story, Mute, Remove Followers, Block, and Unfollow. Main accounts are generally used as more controlled spaces for wider audiences, while alter accounts function as more personal spaces for sharing daily activities, emotional expressions, and spontaneous content with selected audiences.

The findings show that privacy boundaries are formed through audience selection, content limitation, and interaction control. Privacy rules are shaped by relational closeness, gender, situational context, family and environmental norms, and risk consideration. However, these boundaries do not always work as expected. Privacy disturbances still occur through screenshots, screen recordings, reposts, account recommendations, and the detection of restriction practices. Therefore, alter accounts cannot be understood as completely private spaces, but as digital spaces where privacy is continuously negotiated and adjusted.

The logical consequence of these findings for the development of science is that Communication Privacy Management Theory remains relevant for understanding digital privacy practices among Generation Z. This study expands the understanding of privacy management by showing that privacy in social media is not merely a technical matter, but also a social, relational, and cultural process. In the context of Islamic education, these findings can contribute to the development of digital ethics education, especially regarding self-control, responsibility in sharing information, respect for others' privacy, and awareness of the moral consequences of online interaction.

In practice, Islamic education can use these findings to strengthen digital literacy based on ethical and religious values. Students need to be guided not only to use privacy features technically, but also to understand the importance of protecting personal dignity, avoiding the spread of others' private information, and building responsible communication in digital spaces. Thus, privacy management on social media can be connected with Islamic educational values such as amanah, haya', adab, and responsibility. This means that the practice of using Instagram should not only be directed toward self-expression, but also toward ethical awareness, respect for boundaries, and responsible digital behavior.

REFERENCES

- C. Desideria and A. R. Syaki, "Fake Instagram: Manajemen Identitas dan Privasi Melalui Fenomena Finstagram," *Tuturlogi* 3, no. 2 (2022), <https://doi.org/10.21776/ub.tuturlogi.2022.003.02.1>.
- Danah boyd, *It's Complicated: The Social Lives of Networked Teens* (New Haven: Yale University Press, 2014).
- F. A. Annabillah and K. M. Boer, "Fitur Close Friends Instagram sebagai Keterbukaan Diri Mahasiswa yang Mengalami Kecemasan Bermedia Sosial," *Jurnal Indonesia: Manajemen Informatika dan Komunikasi* 4, no. 3 (2023): 1550–1565, <https://doi.org/10.35870/jimik.v4i3.379>.
- F. R. Hidayati and Irwansyah, "Privasi 'Pertemanan' Remaja di Media Sosial," *Jurnal Teknologi dan Sistem Informasi Bisnis* 3, no. 1 (2021): 78–91, <https://doi.org/10.47233/jteksis.v3i1.186>.
- H. Tandres and S. Winduwati, "Pengelolaan Self-Disclosure Generasi Z Melalui Penggunaan Multiple Accounts di Instagram," *Koneksi* 8, no. 1 (2024): 233–244, <https://doi.org/10.24912/kn.v8i1.27659>.
- I. K. C. W. Angga and H. B. Nugroho, "Konstruk Sosial dan Teknologi: Fenomena Penggunaan Fitur Close Friends dalam Second Account Instagram," *Jurnal Riset Komunikasi (Jurkom)* 8, no. 2 (2025): 308–327.
- I. Putri et al., "Media Sosial sebagai Media Pergeseran Interaksi Sosial Remaja," *Jurnal Ilmu Komunikasi Balayudha* 2, no. 2 (2022): 1–10.
- N. Zahrah, S. Suhasman, and M. Akbar, "Pengaruh Second Account Instagram terhadap Pengungkapan Diri dan Manajemen Privasi Generasi Z," *Al-Kalam: Jurnal Komunikasi, Bisnis dan Manajemen* 12, no. 1 (2025), <https://doi.org/10.31602/al-kalam.v12i1.17547>.
- P. W. Aji, P. Utari, and Sudarmo, "Manajemen Privasi Generasi Z dalam Menghadapi Komersialisasi Data Pribadi di Media Sosial," *Jurnal IPTEK-KOM* 24, no. 2 (2022): 103–116.
- S. Tania, "Mengeksplorasi Paradoks Privasi Gen-Z dalam Personalisasi Iklan di Media Digital," *Interaksi: Jurnal Ilmu Komunikasi* 12, no. 1 (2023): 50–65, <https://doi.org/10.14710/interaksi.12.1.50-65>.
- Sandra Petronio and Ashley Hernandez, "Communication Privacy Management Theory," *Oxford Research Encyclopedia of Communication* (2019), <https://doi.org/10.1093/acrefore/9780190228613.013.373>.
- Sandra Petronio, *Boundaries of Privacy: Dialectics of Disclosure* (Albany: State University of New York Press, 2002).
- W. P. Sari and L. Irena, "Model Self-Disclosure Generasi Z Pengguna Berat Media Sosial," *Interaksi: Jurnal Ilmu Komunikasi* 12, no. 1 (2023): 146–164.
- W. Ramadhina et al., "Peranan Media Sosial Instagram terhadap Interaksi Sosial dan Etika pada Generasi Z," *Journal on Education* 6, no. 2 (2024): 11029–11037.
- We Are Social and Meltwater, *Digital 2025: Indonesia* (2025), <https://wearesocial.com>.