Journal of Social Political Sciences
JSPS
Vol. 7, No. 2, May 2026

NEGOTIATING PRIVACY AND INTIMACY: GENERATION Z'S SELF-DISCLOSURE THROUGH INSTAGRAM SECOND ACCOUNTS AND ITS IMPLICATIONS FOR SOCIAL INTERACTION

Syamsiah Badruddin, Paisal Halim, Qonitah Basalamah, Gilang Putra Ramadan
Universitas Nasional Jakarta, Indonesia
Corresponding Author Email: vivitri.andriani@civitas.unas.ac.id

Submission	:	March 13, 2025
Revision	:	April 24, 2026
Publication	:	May 28, 2026

Abstract: This article examines how Generation Z negotiates privacy and intimacy through second accounts on Instagram, and how the self-disclosure practised on those accounts reshapes social interaction. Drawing on five interrelated lenses, Social Penetration Theory, dramaturgical self-presentation, Communication Privacy Management and privacy calculus, context collapse and context restoration, and networked publics, this qualitative interpretive synthesis asks how second accounts facilitate self-disclosure, why they are perceived as safer than primary accounts, and how they reshape closeness, exclusion, support, and validation. The synthesis finds that second accounts function as controlled intimacy spaces: semi-private arenas in which openness is conditioned by audience restriction, privacy calculation, and relational trust. Within those spaces, disclosure becomes deeper and more emotionally expressive, closeness and support can strengthen, yet dependence on peer validation and insider-outsider boundaries also grow. The article argues that privacy on second accounts is therefore not withdrawal from public life but a renegotiation of it, and that the control users exercise remains relative, because intimacy on a commercial platform is still shaped by visibility rules, data extraction, and algorithmic distribution.

Keywords: self-disclosure; Generation Z; Instagram second account; privacy calculus; controlled intimacy spaces; digital social interaction

INTRODUCTION

Social media has become a central infrastructure of everyday life for Generation Z, the cohort that has grown up with platforms as the ordinary setting in which identity is performed, relationships are maintained, and belonging is negotiated (boyd, 2014). Among these platforms, Instagram occupies a distinctive position: it combines visual presentation, narrative storytelling, and networked sociability, so that what users show, and to whom they show it, is itself a social act. Research on why young people use Instagram points to overlapping motives of self-expression, documentation, social interaction, and surveillance of peers (Lee, Lee, Moon, & Sung, 2015; Sheldon & Bryant, 2016). For many young users, however,

a single account cannot carry all of these purposes at once. The primary account, visible to a broad and mixed audience of family, classmates, colleagues, and acquaintances, demands a polished and broadly acceptable self. The second account, by contrast, is typically closed, selective, and restricted to a small circle of trusted followers, and it is there that a more spontaneous, imperfect, humorous, and emotionally open self appears (Huang & Vitak, 2022). This article examines that second account, and asks what it reveals about privacy and intimacy in digital social life.

Indonesian evidence, although still limited, confirms that the second account is a real and patterned practice rather than a marginal curiosity. A phenomenological study of Generation Z in Yogyakarta found that ownership of a second Instagram account has become a phenomenon among young users, that self-disclosure is central to how the account is used, and that reciprocal communication, freedom to share, and perceived similarity between account owner and followers together produce a sense of security (Beatrice & Damastuti, 2024). A study of Generation Z in Baubau City likewise found systematic differences between primary and second accounts in their functions, audiences, content, and the decisions users make about what to disclose (Zayana, Muhammad Hidayatullah, & Muhammad Rizal Ardiansyah Putra, 2025). Together these studies suggest that the second account is best understood not as a hiding place but as a managed social space, and that its analysis requires attention to privacy, presentation, audience, and interaction at the same time.

The first lens used here is Social Penetration Theory, which holds that closeness develops as disclosure grows in depth and breadth, and that people calibrate what they reveal according to safety, reciprocity, and audience control (Altman & Taylor, 1973). On social media, disclosure is further shaped by platform characteristics such as visibility, persistence, shareability, and reach, and by the motivations and functions that disclosure serves for the discloser (Bazarova & Choi, 2014; Cheung, Lee, & Chan, 2015). Research on social media users in Indonesia also shows that self-disclosure is influenced by a combination of personal factors and factors inherent in social media itself (Siahaan, Handayani, & Azzahro, 2021). The question for second accounts is therefore not whether young users disclose, but to whom, in what depth, and under what conditions of safety.

The second lens is dramaturgical self-presentation. In Goffman's (1959) terms, social life is a performance in which a front stage is prepared for a general audience while a backstage allows a more relaxed and less guarded self. The primary account functions as a front stage and the second account as a backstage-like space, yet the second account is not unperformed: its spontaneity is itself curated for a chosen audience. Young users manage an imagined audience, adjusting what they show according to who they believe is watching (Marwick & boyd, 2011; Litt & Hargittai, 2016). Studies of adolescents on Facebook and Instagram confirm that self-presentation is experienced as considerable work, governed by norms about what is appropriate to show, to whom, and in what form (Yau & Reich, 2019). The second account reduces that work by narrowing the audience, but it does not remove the audience.

The third lens combines Communication Privacy Management with privacy calculus. Communication Privacy Management treats private information as governed by boundary rules and by co-ownership: once information is shared, its recipients become co-owners, and boundary turbulence follows when rules are broken (Petronio, 2002). Research on Facebook shows that privacy management is motivated by social concerns and by the perceived consequences of voluntary disclosure (Waters & Ackerman, 2011), and that restricting an audience to friends only is itself a privacy behaviour through which users reclaim control over who sees what (Stutzman & Kramer-Duffield, 2010). Privacy calculus adds the calculation itself: users weigh expected benefits, such as social support, belonging, and emotional release, against perceived risks, such as embarrassment, judgement, conflict, or the spread of information beyond its intended circle (Trepte, Reinecke, Ellison, Quiring, Yao, & Ziegele, 2017; Trepte, 2020). That calculation is not always consistent: attitudes towards privacy and actual privacy behaviour frequently diverge (Dienlin & Trepte, 2014), and the calculation must also take account of others, because disclosure often exposes other people's information as well (Zhang & Zhu, 2025). Platform affordances further condition the calculation, because what a platform makes visible, editable, and distributable shapes what users feel able to disclose (DeVito, Birnholtz, & Hancock, 2017).

The fourth lens is context collapse and context restoration. When family, friends, classmates, and colleagues are merged into a single audience, users face conflicting expectations about what is appropriate, and disclosure becomes riskier (Marwick & boyd, 2011). Collapse takes distinct forms: audiences may be deliberately merged, or they may collide without the user's intention (Davis & Jurgenson, 2014), and the experience of collapse itself shapes whether and how users disclose (Vitak, 2012). Teenagers negotiate this condition not by leaving platforms but by developing practices of networked privacy, managing context within the platform itself (Marwick & boyd, 2014). The second account is one such practice: a strategy of context restoration, in which users separate audiences, adjust content, and rebuild boundaries so that disclosure becomes possible again (Li, Cho, Shen, & Kong, 2023). The fifth lens, networked publics, frames this whole condition: young people do not simply use platforms, they inhabit publics that are structured by the platform's architecture, and they create bounded forms of publicness within it (boyd, 2014).

The literature on these questions remains fragmented. Studies of self-disclosure, of privacy management, and of adolescent peer relations have each advanced part of the picture, but they have rarely been brought together around a single practice, and Indonesian studies of second accounts remain local and descriptive (Beatrice & Damastuti, 2024; Zayana et al., 2025). What is missing is an integrative analysis that follows one practice, the second account, through privacy negotiation, emotional expression, and the reconstruction of social interaction, and that names the concept that holds those processes together. This article proposes controlled intimacy spaces as that concept: semi-private digital arenas in which openness is conditioned by audience restriction, privacy calculation, and relational trust. The

synthesis also attends to platform power, developed in the political analysis section, as a qualifier on the control users exercise. Three research questions guide the analysis. First, how do second accounts facilitate Generation Z's self-disclosure? Second, why are these accounts perceived as safer than primary accounts? Third, how do they reshape social interaction in terms of closeness, exclusion, support, and validation?

LITERATURE REVIEW

Self-Disclosure in Digital Communication

Self-disclosure is the voluntary revelation of personal information, thoughts, and feelings to others, and it is one of the principal mechanisms through which relationships form and deepen. Social Penetration Theory describes this process as movement from superficial to deeper layers of the self, governed by breadth and depth, and it predicts that closeness grows as disclosure becomes more personal and more reciprocal (Altman & Taylor, 1973). On social media, however, disclosure is mediated by platform characteristics that have no offline equivalent: content persists, it can be searched and shared beyond its original audience, and it is visible to people the discloser may not have intended. Disclosure on social media is therefore shaped both by personal factors and by factors inherent in the medium itself, a combination confirmed among Indonesian social media users (Siahaan et al., 2021). A functional approach to disclosure adds that people disclose for distinct reasons, including self-expression, relationship development, social validation, and identity clarification, and that the characteristics of disclosure, its depth, breadth, and honesty, vary with those motivations (Bazarova & Choi, 2014). Research on social networking sites similarly finds that disclosure is driven by anticipated benefits and by trust in the platform and in the audience, and that it carries risks of regret and of unwanted spread (Cheung et al., 2015).

The consequences of disclosure are ambivalent, and the evidence does not support a simple claim that more disclosure is better. A meta-analysis of 38 empirical studies found that the valence and honesty of disclosure, rather than its quantity, were moderately and positively associated with psychological well-being, while the amount of disclosure alone was not significantly associated with well-being, and that these associations were moderated by gender, age, and culture (Chu, Sun, & Jiang, 2023). Supportive responses appear to condition the effect: when disclosure is met with support, it can strengthen well-being, and directed interaction with close ties is the form of online activity most consistently linked to well-being, whereas passive consumption is not (Chu et al., 2023; Burke, Marlow, & Lento, 2010). At the same time, disclosure carries costs that the literature records consistently: misinterpretation, regret, the dissemination of personal information beyond its intended circle, dependence on validation, and conflict when boundaries are crossed, a pattern of risky opportunity that teenagers navigate when they create content for intimacy, privacy, and self-expression (Livingstone, 2008). A narrative review of reviews of teenagers, screens, and social media reaches a similarly cautious conclusion, that effects depend on what young people do online,

with whom, and in what context, rather than on screen time alone (Orben, 2020). A systematic review of social media and adolescent depression, anxiety, and psychological distress likewise finds associations that are real but conditional, and that caution against both alarm and dismissal (Keles, McCrae, & Grealish, 2020). The second account sits inside this ambivalence: it is a setting designed to maximise the benefits of disclosure while minimising its risks, and the question is how far that design succeeds.

Instagram, Generation Z, and Second-Account Practices

Instagram's appeal for young users lies in its visual and narrative character. Motivations for using Instagram include self-expression through images, documentation of everyday life, social interaction, and the surveillance of peers, and the platform's visual logic makes presentation itself a form of communication (Lee et al., 2015). Motives also vary with personality and with contextual age, so that the same platform serves different identity work for different users (Sheldon & Bryant, 2016). For Generation Z, for whom Instagram is a primary social environment rather than a novelty, the management of self-presentation is continuous and demanding: adolescents report that presenting the self on Facebook and Instagram is considerable work, governed by norms about authenticity, effort, and audience (Yau & Reich, 2019). The primary account bears the heaviest burden of that work, because its audience is broad, mixed, and partly unknown, and because its content is expected to be polished and broadly acceptable.

The second account answers that burden by narrowing the audience. In the Yogyakarta study, young users described the second account as a space for freer expression among people they trusted, where reciprocal communication and perceived similarity produced security (Beatrice & Damastuti, 2024). In Baubau City, primary and second accounts differed systematically in function, audience, content, and disclosure decisions: the primary account carried curated, public-facing content, while the second account carried personal, emotional, and everyday content for a selected circle (Zayana et al., 2025). Research on alternative Instagram accounts, often called Finsta and Rinsta accounts, confirms the pattern: the primary account is curated and the alternative account is spontaneous, imperfect, humorous, emotional, and personal, and users move between them according to audience and purpose (Huang & Vitak, 2022). The second account is therefore neither fully public nor fully private. It is a semi-private space, more open than a private message and more closed than a public post, and its interest lies precisely in that intermediate position.

Dramaturgical Self-Presentation and Image Management on Social Media

Goffman's (1959) dramaturgy remains the most economical language for this practice. The primary account is a front stage, prepared for a general audience; the second account resembles a backstage, where the performance can relax. Yet the resemblance is partial. The second account still has an audience, still involves selection and editing, and still responds to norms, and its spontaneity is therefore better described as curated intimacy than as

unguarded authenticity. The imagined audience is central here: users adjust their presentation according to who they believe is watching, and that belief is itself shaped by platform features that make audiences partly visible and partly opaque (Marwick & boyd, 2011; Litt & Hargittai, 2016). Platform affordances matter in the same way: what a platform allows users to show, hide, edit, and distribute shapes how they present themselves and what they feel safe disclosing (DeVito et al., 2017). The second account works dramaturgically because it changes the imagined audience: by restricting followers to trusted others, it changes what counts as an acceptable performance, and so allows a different self to appear.

Communication Privacy Management and Privacy Calculus

Communication Privacy Management provides the privacy language for the same practice. Private information is governed by boundary rules that owners set, and by co-ownership: once information is shared, recipients become co-owners, and boundary turbulence follows when co-owners treat information differently from the way the owner intended (Petronio, 2002). On Facebook, privacy management is motivated by social concerns and by the perceived consequences of voluntary disclosure, so that users manage boundaries not only to protect information but to protect relationships (Waters & Ackerman, 2011). Restricting an audience to friends only is a concrete boundary practice of this kind: it is a privacy-enhancing behaviour through which users reclaim control over who sees what (Stutzman & Kramer-Duffield, 2010). The second account is a boundary practice at the level of the account itself: rather than adjusting the audience of each post, the user creates a separate space with a separate boundary.

Privacy calculus describes the decision that boundary work serves. Users weigh expected benefits, such as social support, belonging, emotional release, and identity expression, against perceived risks, such as embarrassment, judgement, conflict, or the spread of information beyond its intended circle, and they disclose when the balance favours disclosure (Trepte et al., 2017). A privacy model for social media adds that affordances condition this calculation: visibility, persistence, and distribution shape what users perceive as risky and what they perceive as rewarding (Trepte, 2020). The calculation is imperfect. Privacy attitudes and privacy behaviour frequently diverge, so that users who express strong privacy concerns still disclose, and users who disclose still report concern (Dienlin & Trepte, 2014). The calculation must also take account of others: disclosure often exposes other people's information, and a self-other calculus, in which users weigh risks to others as well as to themselves, shapes what they are willing to share (Zhang & Zhu, 2025). The second account does not remove the calculation; it changes its terms, by lowering perceived risk through audience restriction and by raising expected benefit through trust.

Context Collapse, Context Restoration, and Audience Segmentation

Context collapse names the condition that makes the second account necessary. When family, friends, classmates, and colleagues are merged into a single audience, users face conflicting

expectations about what is appropriate, and disclosure becomes riskier (Marwick & boyd, 2011). Collapse takes distinct forms: audiences may be deliberately merged, as when a user accepts followers from different spheres, or they may collide without the user's intention, as when content travels beyond its intended circle (Davis & Jurgenson, 2014). The experience of collapse shapes disclosure itself: when users perceive that their audiences have collapsed, they adjust what they disclose and how they manage privacy (Vitak, 2012). Teenagers respond to this condition with practices of networked privacy, managing context within platforms rather than leaving them (Marwick & boyd, 2014). Audience segmentation is the general name for those practices: dividing audiences, tailoring content, and using platform features to control who sees what.

Context restoration is the constructive counterpart of collapse. Research on how users manage collapsed contexts identifies strategies such as audience separation, content adjustment, and the use of separate spaces, together with the motivations and decision rules that govern when each strategy is chosen (Li et al., 2023). The second account is a restoration strategy at the level of the account: rather than repairing a collapsed audience post by post, the user creates a new, bounded audience from the start. Segmentation of this kind is a form of literacy. It requires users to read audiences, to anticipate how content will travel, and to maintain boundaries over time, and its success depends on trust: on the belief that selected followers will respect the boundary and will not carry content beyond it.

Self-Disclosure, Social Support, and Peer Interaction

The interactional consequences of disclosure are where the literature converges most clearly. Online communication among adolescents strengthens existing friendships when it is used to deepen contact with people already known offline, and it is most beneficial when it supplements rather than replaces face-to-face interaction (Valkenburg & Peter, 2011). Social capital research on Facebook similarly finds that intensity of use is associated with bridging and bonding social capital, and that the benefits flow through interaction with close ties rather than through broadcasting (Ellison, Steinfield, & Lampe, 2007). Directed communication with close ties is the form of online activity most consistently linked to well-being, while passive consumption shows no such association (Burke et al., 2010). The meta-analytic evidence is consistent with this pattern: supportive responses condition whether disclosure relates to well-being, and the valence and honesty of disclosure matter more than its amount (Chu et al., 2023).

Peer relations are also transformed by social media in ways that go beyond support. A theoretical framework for adolescent peer relations in the social media context identifies transformation in the frequency, quality, and public character of peer interaction, including new forms of validation, exclusion, and norm enforcement (Nesi, Choukas-Bradley, & Prinstein, 2018). Validation becomes visible and countable, through likes, comments, and replies, and young users learn to read those signals as evidence of acceptance or rejection.

Norm enforcement also becomes networked: peers reinforce norms not only face to face but through public responses, and morally motivated harassment can function as a form of normative reinforcement within a network (Marwick, 2021). Adolescent mental health in the digital age must therefore be understood in these interactional terms: effects are not produced by platforms in the abstract but by specific patterns of interaction, including support, validation, exclusion, and conflict, within specific relationships (Odgers & Jensen, 2020). The second account concentrates these dynamics: it intensifies closeness and support within a selected circle, and it sharpens the boundary between those inside and those outside it.

Controlled Intimacy Spaces as a Conceptual Framework

Controlled intimacy spaces names the synthesis of these lenses. A controlled intimacy space is a semi-private digital arena in which openness is conditioned by three things together: audience restriction, privacy calculation, and relational trust. Audience restriction is the structural condition: the space exists because its audience has been narrowed. Privacy calculation is the decision process: users disclose when expected benefits outweigh perceived risks, including risks to others. Relational trust is the social condition: the space works only when selected followers are believed to respect its boundaries. The concept integrates the five lenses rather than replacing them. Social Penetration Theory supplies the mechanism of closeness through depth and breadth; dramaturgy supplies the performance logic of front stage and backstage-like presentation; Communication Privacy Management supplies the boundary rules and the risk of turbulence; privacy calculus supplies the benefit-risk decision; context collapse and restoration supply the problem and the strategy; and networked publics supply the setting in which bounded publicness is created. Figure 1 summarises the framework, and Table 1 states, for each lens, what would count in the reviewed literature as evidence for it, and where in this article it is used.

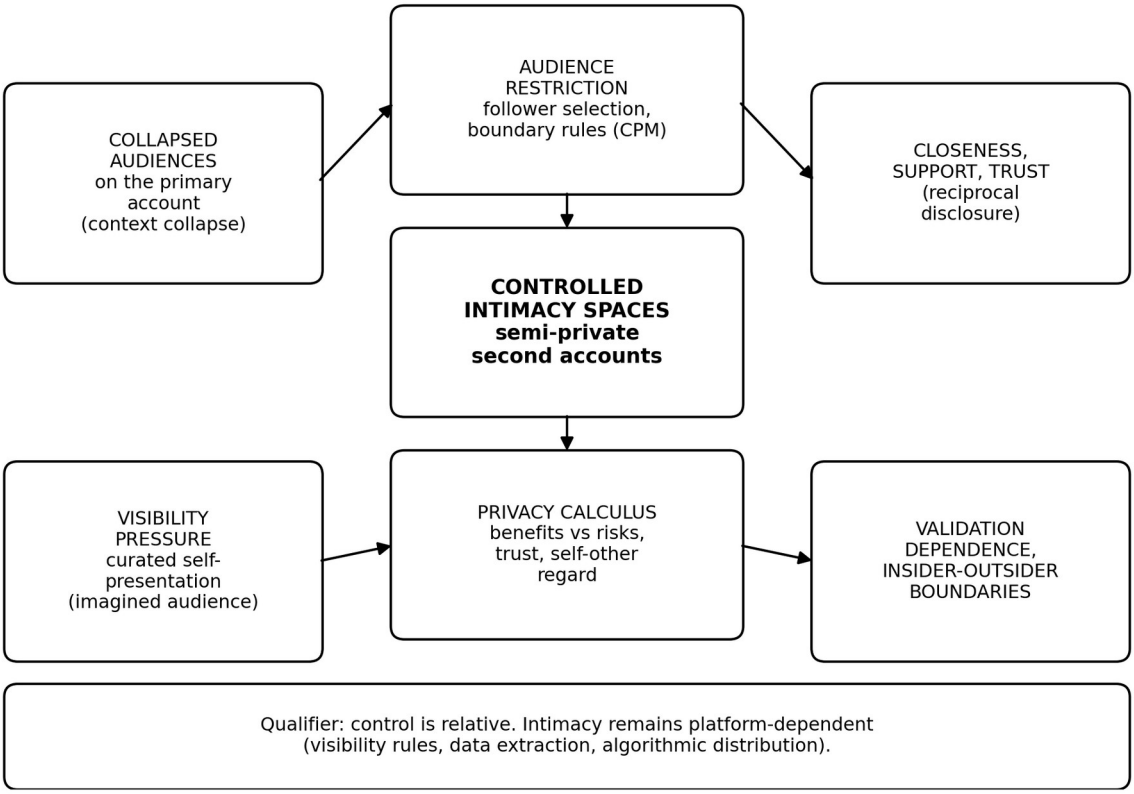


Figure 1. Controlled intimacy spaces: how collapsed audiences and visibility pressure lead, through audience restriction and privacy calculus, to ambivalent outcomes.

Source: Author-built diagram from the framework lenses used in this article. It is not copied from any source and contains no generated imagery.

Lens	Proposition in this article	Indicator in the reviewed literature	Where used
Social Penetration Theory	Closeness grows with depth and breadth of disclosure to trusted others	Deeper, more personal disclosure directed to selected followers; reciprocal openness	Introduction; Literature Review; Results; Conclusion (RQ1)
Dramaturgical self-presentation	Primary account as front stage; second account as backstage-like, still curated	Curated versus relaxed presentation by account; imagined-audience management	Introduction; Literature Review; Results
Communication Privacy Management	Private information governed by boundary rules and co-ownership	Follower selection and access rules; trust norms; leakage as boundary turbulence	Introduction; Literature Review; Results (RQ2)
Privacy calculus (including self-other calculus)	Disclosure follows perceived benefits versus risks, including risks to others	Benefit-risk statements; venting involving others flagged as relational risk	Introduction; Literature Review; Results (RQ2)
Context collapse and	Merged audiences	Audience separation	Introduction; Literature

restoration	pressure users; second accounts restore boundaries	strategies; creation of bounded spaces	Review; Results (RQ2, RQ3)
Networked publics	Youth create bounded publicness within platforms rather than leaving them	Selective participation in peer publics; bounded rather than open visibility	Introduction; Literature Review; Synthesis
Qualifier: platform dependence	Control is relative; intimacy remains shaped by platform power	Visibility rules, data extraction, and algorithmic distribution as constraints	Political analysis section; Synthesis

Two clarifications matter. First, controlled intimacy spaces is a concept for describing a practice, not a claim that control is complete. The qualifier in Figure 1 and Table 1 is part of the concept, not an afterthought: the same platform that allows audience restriction also sets the rules of visibility, extracts data, and distributes content algorithmically, and those conditions limit the control users exercise. The political analysis section develops this qualifier. Second, the concept is presented as a synthesis of the reviewed literature, not as an empirically tested model. It organises what the literature shows, and it generates expectations that future empirical work, through interviews, digital ethnography, surveys, or mixed methods, could test. That limitation is stated plainly in the Method and in the Novelty and Limitations section, and it is the reason the article's claims are framed as interpretive rather than causal.

METHOD

This study uses a qualitative interpretive synthesis of secondary literature. Its orientation is scoping in the sense described by Arksey and O'Malley (2005): it maps the key concepts, the available evidence, and the gaps in a body of literature, rather than testing a single hypothesis. The synthesis is interpretive rather than procedural in a stronger sense, and that distinction is stated plainly here because it governs how the findings should be read. No pre-registered protocol is reported, no databases are named, no search dates or date range are reported, and no numbers of screened or included sources are reported, because the search record underlying this article was not available to it. The study is therefore presented as a thematic synthesis of the secondary literature, not as a structured scoping review with a reproducible search protocol, and no corpus count is claimed.

The corpus consists of secondary sources: peer-reviewed articles, conference proceedings, books, and reports that address at least one of four topical areas: self-disclosure on social media; Instagram use and second-account practices among Generation Z; privacy management, privacy calculus, and audience segmentation; and social interaction, support, validation, and exclusion in digital peer relations. The search keywords used were self-disclosure, Instagram second account, Generation Z, privacy calculus, communication privacy management, context collapse, audience management, digital intimacy, and social interaction. No exclusion criteria beyond topical relevance are claimed, and no formal quality

appraisal step is claimed. Sources were read for what they show about the practice of second accounts and about the lenses through which that practice can be understood, and Indonesian studies were given particular weight where the question concerned the Indonesian context, because the literature on second accounts in Indonesia remains thin.

Analysis followed three stages, following the thematic approach described by Braun and Clarke (2006). First, sources were read repeatedly and initial themes were identified across them. Second, themes were grouped into categories corresponding to the article's questions: facilitation of disclosure, perceived safety, and reshaping of interaction. Third, the categories were interpreted through the five lenses, Social Penetration Theory, dramaturgy, Communication Privacy Management and privacy calculus, context collapse and restoration, and networked publics, and the integrative concept of controlled intimacy spaces was formulated from that interpretation. The political analysis was developed as a further interpretive step, reading the same practice through platform power, and its conclusions are presented as a qualifier on user control rather than as a separate theory.

Five limitations are stated here and carried through the article. First, the study relies entirely on secondary literature and contains no direct empirical data: no interviews, surveys, or observations were conducted. Second, Indonesia-specific literature on second accounts is thin, so that claims about the Indonesian context rest on a small number of studies. Third, the synthesis concerns Instagram only, and its conclusions do not automatically extend to other platforms. Fourth, the reviewed literature does not allow systematic differentiation by gender, class, location, or culture, and the synthesis therefore does not claim such differences. Fifth, the concept of controlled intimacy spaces is untested: it organises the reviewed literature, but it has not been validated against primary data, and future work using interviews, digital ethnography, surveys, or mixed methods is needed to test it. A sixth limitation concerns reporting itself: because no search log is available, the synthesis cannot be reproduced as a search, and readers should treat its coverage as interpretive mapping rather than as an exhaustive review.

RESULTS AND DISCUSSION

The Use of Instagram Second Accounts as a Medium of Self-Disclosure

Second accounts facilitate self-disclosure by changing the conditions under which disclosure happens, not by changing the desire to disclose. The primary account constrains disclosure through a broad and mixed audience: family, friends, classmates, and colleagues see the same content, and the user must produce a self that is acceptable to all of them at once. The second account removes that constraint by narrowing the audience to trusted followers, and disclosure that would be risky on the primary account becomes possible there. In the Yogyakarta study, young users described the second account as a space where they could share freely, where reciprocal communication was expected, and where perceived similarity with followers produced security (Beatrice & Damastuti, 2024). In Baubau City, the difference

was systematic: primary accounts carried curated, public-facing content, while second accounts carried personal, emotional, and everyday content, and users made different disclosure decisions on each account according to audience and purpose (Zayana et al., 2025). Research on alternative Instagram accounts confirms the same division: the primary account is curated, while the alternative account is spontaneous, imperfect, humorous, emotional, and personal (Huang & Vitak, 2022).

Social Penetration Theory explains why the change of audience changes disclosure. Closeness develops as disclosure grows in depth and breadth, and people calibrate what they reveal according to safety, reciprocity, and audience control (Altman & Taylor, 1973). On the primary account, safety is low because the audience is mixed, and so depth stays shallow. On the second account, safety is higher because the audience is selected, and so depth increases: users share feelings, difficulties, and everyday struggles that they would not share publicly. The functional approach to disclosure adds that this deeper disclosure serves distinct purposes, including self-expression, relationship development, and identity clarification, and that its characteristics vary with those purposes (Bazarova & Choi, 2014). Adolescents' experience of self-presentation as considerable work, governed by norms about what is appropriate to show and to whom (Yau & Reich, 2019), explains why the second account is experienced as relief: it does not abolish the work of presentation, but it changes the norms that govern it, so that a more relaxed performance becomes acceptable. Dramaturgically, the second account is a backstage-like space, but its spontaneity remains curated for its chosen audience (Goffman, 1959). The facilitation of disclosure is therefore real but conditional: second accounts facilitate disclosure by narrowing the audience, and the disclosure they facilitate is deeper, more emotional, and more reciprocal than disclosure on the primary account, but it remains a performance for an audience, not an escape from audiences altogether.

Perceived Safety in the Use of Second Accounts

Second accounts are perceived as safer than primary accounts for three connected reasons: audience restriction, privacy calculation, and relational trust. Audience restriction is the structural reason. By selecting followers, users create a boundary that the primary account lacks, and that boundary is itself a privacy behaviour: restricting an audience to trusted others is a way of reclaiming control over who sees what (Stutzman & Kramer-Duffield, 2010). Communication Privacy Management describes the logic: private information is governed by boundary rules, and once information is shared its recipients become co-owners, so that safety depends on whether co-owners respect the rules (Petronio, 2002). On Facebook, privacy management is motivated by social concerns and by the perceived consequences of voluntary disclosure, which means that users manage boundaries to protect relationships as much as to protect information (Waters & Ackerman, 2011). The second account institutionalises that logic at the level of the account: the boundary is set once, by follower selection, rather than negotiated post by post.

Privacy calculation is the decision reason. Users weigh expected benefits, such as social support, belonging, and emotional release, against perceived risks, such as embarrassment, judgement, conflict, or the spread of information beyond its intended circle, and they disclose when the balance favours disclosure (Trepte et al., 2017). A privacy model for social media adds that affordances condition the calculation, because visibility, persistence, and distribution shape what users perceive as risky and what they perceive as rewarding (Trepte, 2020). On the second account, perceived risk falls because the audience is smaller and more trusted, while expected benefit rises because support and understanding are more likely, and the balance therefore shifts towards disclosure. The calculation is imperfect: privacy attitudes and privacy behaviour frequently diverge, so that users who express strong privacy concerns still disclose (Dienlin & Trepte, 2014). It must also take account of others: disclosure often exposes other people's information, and users weigh risks to others as well as to themselves when deciding what to share (Zhang & Zhu, 2025). In Indonesia, disclosure is influenced by a combination of personal factors and factors inherent in social media itself (Siahaan et al., 2021), and the second account works because it changes the media factors, audience size and composition, in the user's favour.

Relational trust is the social reason, and it is the one on which safety most depends. The Yogyakarta study found that reciprocal communication, freedom to share, and perceived similarity together produced security, which suggests that safety is not a property of the account but of the relationships within it (Beatrice & Damastuti, 2024). In Baubau City, disclosure decisions differed by account precisely because the audiences differed in trust (Zayana et al., 2025). The critical reading follows from this: perceived safety is not the same as actual safety. A second account is still on a commercial platform, its content can be screenshotted and carried beyond its boundary, and trust can be broken. Boundary turbulence, in Petronio's (2002) terms, remains possible, and when it happens the harm can be greater precisely because the disclosure was deeper. Second accounts are therefore perceived as safer for good reasons, audience restriction, a favourable privacy calculation, and relational trust, but that safety is conditional and revocable, and the perception of safety should not be mistaken for a guarantee.

Privacy Negotiation, Audience Segmentation, and Context Restoration

Privacy negotiation on second accounts is continuous, not a single decision. Users select followers, adjust what they share, withdraw content, and monitor who remains inside the boundary, and each of these acts is a negotiation between the desire to disclose and the need to control. Context collapse is the condition that makes negotiation necessary: when family, friends, classmates, and colleagues are merged into a single audience, conflicting expectations make disclosure riskier (Marwick & boyd, 2011). Collapse takes distinct forms, deliberate merging and unintended collision (Davis & Jurgenson, 2014), and the experience of collapse shapes whether and how users disclose (Vitak, 2012). Teenagers respond with practices of networked privacy, managing context within platforms rather than leaving them (Marwick &

boyd, 2014), and the second account is the most complete form of that response: rather than repairing a collapsed audience post by post, the user creates a new, bounded audience from the start. Research on context restoration identifies strategies such as audience separation, content adjustment, and the use of separate spaces, together with the motivations and decision rules that govern when each strategy is chosen (Li et al., 2023), and the second account embodies the separation strategy in its strongest form.

Segmentation has consequences that go beyond the individual user. When audiences are divided, information flows are divided too: what the selected circle knows, the wider circle does not, and the boundary between them becomes a social fact. This is where the insider-outsider dynamic begins. Those inside the second account share knowledge, jokes, and emotional history that those outside do not, and that shared knowledge becomes a marker of closeness. Peer relations are transformed by exactly this kind of dynamic: social media changes the frequency, quality, and public character of peer interaction, including new forms of validation, exclusion, and norm enforcement (Nesi et al., 2018). Segmentation is therefore not only a privacy technique; it is a social technique, and its success depends on trust that the boundary will be respected. When that trust holds, segmentation enables disclosure; when it fails, the same boundary that enabled disclosure becomes the channel through which private content travels.

The Impact of Self-Disclosure on Social Interaction

The impact of second-account disclosure on social interaction is ambivalent, and the synthesis finds both strengthening and straining effects. On the strengthening side, disclosure on second accounts deepens closeness. Social Penetration Theory predicts that closeness grows as disclosure becomes deeper and more reciprocal (Altman & Taylor, 1973), and the second account creates the conditions for that growth: a selected audience, deeper content, and reciprocal openness. Online communication among adolescents strengthens existing friendships when it deepens contact with people already known offline (Valkenburg & Peter, 2011), and social capital research finds that the benefits of online interaction flow through interaction with close ties rather than through broadcasting (Ellison et al., 2007). Directed communication with close ties is the form of online activity most consistently linked to well-being (Burke et al., 2010), and the meta-analytic evidence is consistent: supportive responses condition whether disclosure relates to well-being, and the valence and honesty of disclosure matter more than its amount (Chu et al., 2023). The second account concentrates exactly these conditions: directed, honest, emotionally expressive disclosure to close ties, met with support. Closeness and support can therefore genuinely strengthen.

On the straining side, the same dynamics produce dependence and exclusion. Validation becomes visible and countable, through likes, comments, and replies, and young users learn to read those signals as evidence of acceptance or rejection. Peer relations are transformed in this way: validation, exclusion, and norm enforcement take new, networked forms (Nesi et al.,

2018), and peers reinforce norms through public responses, including morally motivated responses that function as normative reinforcement within a network (Marwick, 2021). When support is expected and does not arrive, or when a post is seen but not acknowledged, the same space that offered closeness can produce hurt. Exclusion is the counterpart of selection: those outside the second account may know that a second account exists without knowing its content, and that knowledge itself can strain relationships, producing feelings of being left out or distrusted. The literature on adolescent mental health in the digital age cautions against attributing these effects to platforms in the abstract: effects are produced by specific patterns of interaction, including support, validation, exclusion, and conflict, within specific relationships (Odgers & Jensen, 2020). The second account does not resolve that ambivalence; it concentrates it, intensifying both closeness within the selected circle and distance from those outside it.

Controlled Intimacy Spaces as a Synthesis of Findings

Controlled intimacy spaces synthesises these findings. The concept holds together because each lens contributes one element and no lens alone is sufficient. Audience restriction, from Communication Privacy Management and from context restoration, explains the structure. Privacy calculation, from privacy calculus, explains the decision. Relational trust, from Social Penetration Theory and from the Indonesian studies, explains why the structure works when it works. Dramaturgy explains why the disclosure that results is still a performance, and networked publics explains why the practice takes the form of bounded publicness rather than withdrawal. Figure 1 and Table 1 state this integration explicitly, so that the concept can be examined rather than merely asserted. The qualifier is part of the concept: control is relative, because the platform sets the rules of visibility, extracts data, and distributes content algorithmically, and the political analysis that follows develops that qualifier. The synthesis therefore answers the three research questions together: second accounts facilitate disclosure by narrowing the audience and so changing the privacy calculation; they are perceived as safer because audience restriction, a favourable calculation, and relational trust together lower perceived risk; and they reshape interaction by intensifying closeness and support within a selected circle while sharpening validation dependence and insider-outsider boundaries.

Political Perspective Analysis: Platform Power, Privacy, and Digital Citizenship

The analysis so far has treated the second account as a user strategy, and that treatment is incomplete without its political dimension. The second account is also a micro-political strategy: a way in which young users negotiate power within a platform that they do not own and do not govern. Users cannot change the platform's rules, its data practices, or its algorithmic distribution, but they can change their own position within those rules by creating a bounded space. That act is political in a modest but real sense: it asserts a claim to control over audience and visibility against a platform architecture that defaults to openness

and spread. The claim is partial, because the platform retains the final say over what is visible, to whom, and for how long, but it is not empty, because audience restriction does change what other users see, and therefore changes the social consequences of disclosure.

Surveillance capitalism provides the structural context for that claim. Platforms extract behavioural data, predict behaviour, and monetise attention, so that user activity, including intimate disclosure, becomes raw material for commercial purposes (Zuboff, 2019). Within that structure, the rules that govern content are set by platforms themselves, through moderation systems and community standards that are only partly transparent and that users cannot negotiate (Gillespie, 2018). Moderation at scale compounds the problem: when platforms must govern vast quantities of content, decisions are made through automated systems and opaque procedures, and users experience governance as distant and unaccountable (Gillespie, 2020). The second account does not escape this structure. Its content is still hosted, processed, and potentially distributed by the platform, and its privacy is therefore conditional on platform practices that users cannot see or control.

Algorithmic power adds a further dimension. Platforms do not merely host content; they distribute it, rank it, and make it visible or invisible according to algorithmic logics that users only partly understand (Bucher, 2012). Influence on platforms is negotiated through a visibility game, in which users and algorithms together determine what is seen (Cotter, 2019), and that game is structured by a social media logic in which programmability, popularity, connectivity, and datafication shape what circulates (Van Dijck & Poell, 2013). Platformisation, the process by which platforms extend their infrastructures and logics into social life, means that even intimate practices such as second-account disclosure take place within platform conditions (Poell, Nieborg, & Van Dijck, 2019). The second account is therefore best described as a controlled but platform-dependent intimacy space: controlled, because users do restrict audiences and do manage boundaries, but platform-dependent, because the space itself exists on terms set by the platform.

Digital citizenship follows from this analysis. If privacy is a matter of citizenship as well as of individual choice, then the governance of platforms becomes a public question, not only a private one. Users need audience transparency, so that they can see who can see their content and how it travels. They need algorithmic accountability, so that distribution decisions that affect intimate content are explainable and contestable. They need protection from manipulative design, so that platforms cannot engineer disclosure through defaults and nudges that users do not understand. And they need meaningful control, not only formal settings, so that boundary decisions users make are respected in practice. Digital literacy, in this framing, is not only a technical skill but a critical awareness: the ability to read platform power, to anticipate how content travels, and to make informed decisions about disclosure. The second account shows both the possibility and the limit of that literacy: young users already practise sophisticated boundary management, but they practise it within a structure

they do not govern, and the task of governance is to make that structure more accountable to them.

Theoretical Implications

Three theoretical implications follow. First, the analysis shows that self-disclosure on social media cannot be understood through a single lens. Depth and breadth, performance, boundary rules, calculation, collapse and restoration, and networked publics each capture part of the practice, and the second account is interesting precisely because it requires all of them at once. A theory of digital disclosure that omits any one of these lenses will misdescribe the practice, either by treating it as purely psychological, purely performative, or purely technical. Second, the analysis integrates Social Penetration Theory with Communication Privacy Management and privacy calculus in a way that neither theory achieves alone. Social Penetration Theory explains why disclosure deepens closeness, but it does not explain boundary work; Communication Privacy Management explains boundary work, but it does not explain the benefit-risk decision; privacy calculus explains the decision, but it does not explain the social conditions of trust. Together, they explain why second accounts work when they work and why they fail when trust breaks. Third, the analysis extends context restoration beyond a technical strategy. Restoration is usually described as audience management, but the second account shows that restoration is also a social act: it creates a space with its own norms, its own history, and its own insider-outsider boundary, and that space then reshapes the relationships within it. The concept of controlled intimacy spaces is offered as a way of holding these three implications together, and it is applicable beyond second accounts, to any bounded digital space in which disclosure is conditioned by audience restriction, calculation, and trust, including close-friends lists, private groups, and alternative accounts on other platforms.

Practical Implications

For educators and universities, the implication is that digital literacy education should go beyond cybersecurity and misinformation to include boundary management, emotional disclosure, and audience awareness. Students already practise boundary management, but they do so without a vocabulary for it, and without systematic attention to validation risks and to the consequences of exclusion. Curricula that teach students to read audiences, to anticipate how content travels, and to recognise when disclosure is driven by validation rather than by trust would build on practices students already have, rather than treating those practices as problems to be corrected. For mental health practitioners and counsellors, the implication is that second accounts should not be treated as immediately negative or deceptive. They serve support functions, and they can be resources for young people who need a space to express difficulty. Practitioners should attend instead to the risks that the synthesis identifies: dependence on validation, exclusion of those outside the circle, and conflict when trust is broken or content travels beyond its boundary. For platform policymakers and

governance, the implication is that relational privacy deserves the same attention as informational privacy. Design that supports selective sharing, audience clarity, and boundary management, and governance that makes distribution decisions transparent and contestable, would support the practices young users already value, rather than treating privacy as a setting to be toggled.

Novelty and Limitations

The novelty of this article lies in its integration. It brings together five lenses that are usually treated separately, applies them to a single practice, and formulates a concept, controlled intimacy spaces, that organises the findings and generates testable expectations. The concept is presented as a synthesis of the reviewed literature, and its value will be judged by whether future empirical work finds it useful. The limitations are stated in the Method and repeated here in summary because they govern how the conclusions should be read. The study relies entirely on secondary literature and contains no direct empirical data. Indonesia-specific literature on second accounts is thin. The synthesis concerns Instagram only. The reviewed literature does not allow systematic differentiation by gender, class, location, or culture. The concept is untested against primary data. And because no search log is available, the synthesis is interpretive mapping rather than a reproducible review. These limitations do not invalidate the synthesis, but they do mean that its claims should be read as interpretive and provisional, and that empirical testing is the necessary next step.

CONCLUSION

This article asked three research questions about Generation Z's second accounts on Instagram, and each can now be answered. First, how do second accounts facilitate self-disclosure? They facilitate disclosure by narrowing the audience and so changing the conditions of disclosure: depth increases, emotional expression becomes possible, and reciprocal openness develops, because safety, in the sense of audience restriction and relational trust, is higher than on the primary account. Second, why are these accounts perceived as safer than primary accounts? They are perceived as safer for three connected reasons: audience restriction creates a boundary that the primary account lacks; the privacy calculation shifts in the user's favour, because perceived risk falls while expected benefit rises; and relational trust, built through reciprocal communication and perceived similarity, makes the boundary credible. That safety is conditional and revocable, because content can travel beyond its boundary and trust can be broken, but the perception of safety rests on real structural and social grounds. Third, how do second accounts reshape social interaction in terms of closeness, exclusion, support, and validation? They intensify closeness and support within a selected circle, because directed, honest, emotionally expressive disclosure to close ties is the pattern most consistently linked to well-being and to social capital. At the same time, they sharpen validation dependence, because support becomes visible and countable, and they sharpen insider-outsider boundaries, because what the selected circle knows, the

wider circle does not. The net effect is ambivalent: stronger bonds inside the space, and greater distance from those outside it.

The contribution of the article is the concept of controlled intimacy spaces, which holds these answers together. Privacy on second accounts is not withdrawal from public life but a renegotiation of it: users do not leave the platform, they create bounded publicness within it, and they do so by combining audience restriction, privacy calculation, and relational trust. That control is relative, because intimacy on a commercial platform remains shaped by visibility rules, data extraction, and algorithmic distribution, and the political analysis of platform power is therefore part of the concept rather than an addition to it. Future research should test the concept empirically, through interviews, digital ethnography, surveys, and mixed methods, and should compare second-account practices by gender, class, location, and culture, and across platforms, where this synthesis could not. Three recommendations follow from the findings. First, digital literacy curricula should teach boundary management, audience awareness, and validation risks, building on practices students already have. Second, practitioners should treat second accounts as support spaces while monitoring validation dependence, exclusion, and trust-breach conflict. Third, platform governance should provide audience transparency, selective-sharing and boundary-management design, and algorithmic accountability, so that the control users already exercise is respected in practice rather than undermined by design.

Second accounts will not resolve the tensions of digital social life, and they are not presented here as a solution. They are a practice through which young users negotiate those tensions day by day, and they deserve analysis that takes both their ingenuity and their limits seriously. The controlled intimacy space is a useful name for that practice, because it captures what users achieve, a space in which intimacy becomes possible, and what they cannot achieve alone, a space fully under their control. Privacy, in this account, is not a setting but a relationship: negotiated with audiences, calculated against risks, sustained by trust, and constrained by platforms. Understanding it in those terms is the task that this synthesis has begun, and that empirical work must continue.

REFERENCES

Altman, I., & Taylor, D. A. (1973). Social penetration: The development of interpersonal relationships. Holt, Rinehart & Winston.

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. International Journal of Social Research Methodology, 8(1), 19-32. https://doi.org/10.1080/1364557032000119616

Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. Journal of Communication, 64(4), 635-657. https://doi.org/10.1111/jcom.12106

Beatrice, V. A., & Damastuti, R. (2024). Phenomenon of self disclosure in use second Instagram account, study phenomenology of Gen-Z in Yogyakarta. International Conference on Communication and Media Digital, 1(1), 169-180.

boyd, d. (2014). It's complicated: The social lives of networked teens. Yale University Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Bucher, T. (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. New Media & Society, 14(7), 1164-1180. https://doi.org/10.1177/1461444812440159

Burke, M., Marlow, C., & Lento, T. (2010). Social network activity and social well-being. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1909-1912. https://doi.org/10.1145/1753326.1753613

Cheung, C. M. K., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites. Internet Research, 25(2), 279-299. https://doi.org/10.1108/IntR-09-2013-0192

Chu, T. H., Sun, M., & Jiang, L. C. (2023). Self-disclosure in social media and psychological well-being: A meta-analysis. Journal of Social and Personal Relationships, 40(2), 576-599. https://doi.org/10.1177/02654075221119429

Cotter, K. (2019). Playing the visibility game: How digital influencers and algorithms negotiate influence on Instagram. New Media & Society, 21(4), 895-913. https://doi.org/10.1177/1461444818815684

Davis, J. L., & Jurgenson, N. (2014). Context collapse: Theorizing context collusions and collisions. Information, Communication & Society, 17(4), 476-485. https://doi.org/10.1080/1369118X.2014.888458

DeVito, M. A., Birnholtz, J., & Hancock, J. T. (2017). Platforms, people, and perception. Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, 740-754. https://doi.org/10.1145/2998181.2998192

Dienlin, T., & Trepte, S. (2014). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285-297. https://doi.org/10.1002/ejsp.2049

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12(4), 1143-1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.

Gillespie, T. (2020). Content moderation, AI, and the question of scale. Big Data & Society, 7(2). https://doi.org/10.1177/2053951720943234

Goffman, E. (1959). The presentation of self in everyday life. Doubleday.

Huang, X., & Vitak, J. (2022). "Finsta gets all my bad pictures": Instagram users' self-presentation across Finsta and Rinsta. Proceedings of the ACM on Human-Computer Interaction, 6(CSCW1), 1-25. https://doi.org/10.1145/3512916

Keles, B., McCrae, N., & Grealish, A. (2020). A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents. International Journal of Adolescence and Youth, 25(1), 79-93. https://doi.org/10.1080/02673843.2019.1590851

Lee, E., Lee, J.-A., Moon, J. H., & Sung, Y. (2015). Pictures speak louder than words: Motivations for using Instagram. Cyberpsychology, Behavior, and Social Networking, 18(9), 552-556. https://doi.org/10.1089/cyber.2015.0157

Li, P., Cho, H., Shen, C., & Kong, H. (2023). From context adaptation to context restoration: Strategies, motivations, and decision rules of managing context collapse on WeChat. Journal of Computer-Mediated Communication, 29(1). https://doi.org/10.1093/jcmc/zmad043

Litt, E., & Hargittai, E. (2016). The imagined audience on social network sites. Social Media + Society, 2(1). https://doi.org/10.1177/2056305116633482

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. New Media & Society, 10(3), 393-411. https://doi.org/10.1177/1461444808089415

Marwick, A. E. (2021). Morally motivated networked harassment as normative reinforcement. Social Media + Society, 7(2). https://doi.org/10.1177/20563051211021378

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. New Media & Society, 13(1), 114-133. https://doi.org/10.1177/1461444810365313

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16(7), 1051-1067. https://doi.org/10.1177/1461444814543995

Nesi, J., Choukas-Bradley, S., & Prinstein, M. J. (2018). Transformation of adolescent peer relations in the social media context: Part 1: A theoretical framework and application to dyadic peer relationships. Clinical Child and Family Psychology Review, 21(3), 267-294. https://doi.org/10.1007/s10567-018-0261-x

Odgers, C. L., & Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. Journal of Child Psychology and Psychiatry, 61(3), 336-348. https://doi.org/10.1111/jcpp.13190

Orben, A. (2020). Teenagers, screens and social media: A narrative review of reviews and key studies. Social Psychiatry and Psychiatric Epidemiology, 55(4), 407-414. https://doi.org/10.1007/s00127-019-01825-4

Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. State University of New York Press.

Poell, T., Nieborg, D., & Van Dijck, J. (2019). Platformisation. Internet Policy Review, 8(4). https://doi.org/10.14763/2019.4.1425

Sheldon, P., & Bryant, K. (2016). Instagram: Motives for its use and relationship to narcissism and contextual age. Computers in Human Behavior, 58, 89-97. https://doi.org/10.1016/j.chb.2015.12.059

Siahaan, M. N., Handayani, P. W., & Azzahro, F. (2021). Self-disclosure of social media users in Indonesia: The influence of personal and social media factors. Information Technology & People, 35(7), 1931-1954. https://doi.org/10.1108/itp-06-2020-0389

Stutzman, F., & Kramer-Duffield, J. (2010). Friends only. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1553-1562. https://doi.org/10.1145/1753326.1753559

Trepte, S. (2020). The social media privacy model: Privacy and communication in the light of social media affordances. Communication Theory, 31(4), 549-570. https://doi.org/10.1093/ct/qtz035

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. Social Media + Society, 3(1). https://doi.org/10.1177/2056305116688035

Valkenburg, P. M., & Peter, J. (2011). Online communication among adolescents: An integrated model of its attraction, opportunities, and risks. Journal of Adolescent Health, 48(2), 121-127. https://doi.org/10.1016/j.jadohealth.2010.08.020

Van Dijck, J., & Poell, T. (2013). Understanding social media logic. Media and Communication, 1(1), 2-14. https://doi.org/10.17645/mac.v1i1.70

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. Journal of Broadcasting & Electronic Media, 56(4), 451-470. https://doi.org/10.1080/08838151.2012.732140

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. Journal of Computer-Mediated Communication, 17(1), 101-115. https://doi.org/10.1111/j.1083-6101.2011.01559.x

Yau, J. C., & Reich, S. M. (2019). "It's just a lot of work": Adolescents' self-presentation norms and practices on Facebook and Instagram. Journal of Research on Adolescence, 29(1), 196-209. https://doi.org/10.1111/jora.12376

Zayana, Muhammad Hidayatullah, & Muhammad Rizal Ardiansyah Putra (2025). Analysis of main account versus second account Instagram as a media for self-disclosure of Generation Z in Baubau City. Mediakita, 9(2), 270-289. https://doi.org/10.30762/mediakita.v9i2.2936

Zhang, M., & Zhu, H. (2025). "Their privacy matters too!": A self-other calculus perspective on disclosure of others' information on social media. Computers in Human Behavior, 165, 108512. https://doi.org/10.1016/j.chb.2025.108665

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.