

Shielding Communication Privacy: Unveiling The Strategic Utilization Of Instagram's Second Account Feature By Millennial Generation

Musfiah Saidah

UIN Syarif Hidayatullah Jakarta, Tangerang Selatan, Indonesia

E-mail: musfiah.saidah@uinjkt.ac.id

Abstract: *Privacy management amid the development of social media seems to be in a dilemma. On the one hand, social media provides space for expression and self-expression, including all information that comes in a personal context. But on the otherhand this has the potential to violate privacy. Uniquely, the second account feature is often considered a safe zone to express oneself more openly. It is in such situations that management privacy is required. In the theory of communication privacy management (CPM) by Sandra Petronio, a person's boundaries in behavior must be determined by himself. This research uses a qualitative approach with a case study method. Data collection techniques by interviewing and documenting several uploads on the informant's second account. The results of this study indicate that the various violations that occurred on the second account were caused by a lack of knowledge to a wrong understanding that the data would be stored safely with the closest trusted person. Even though the person who is selected to enter the second account circle is also vulnerable to opening the data privacy of the account owner and even spreading it. After this research is expected to be input for social media users to be wiser in managing their privacy even in features that are considered safe.*

Keywords: *Privacy, Instagram, Second Account, and Millennials.*

Article Info:

Received 23 March 2023 , Revised 30 June 2023, Accepted 3 July 2023, Available online 6 July 2023

INTRODUCTION

Issues around privacy in the digital era seem to be faced with the phenomenon of freedom of expression without control, thus opening up opportunities for personal data to open. On the one hand, social media can be a means of communication. But on the other hand, the desire to share personal information makes privacy boundaries even more biased (Roessler, B., & Mokrosinska, 2013). Social media can encourage someone to share personal information intentionally without considering the impact. Even though every upload will be recorded as a digital footprint. By being more conscious of their online participation, consumers can take responsibility for fixing the aforementioned issues (Koidl et al., 2018). Therefore it is important that social media users need to be wise in

treating their personal data.

The phenomenon of sharing whereabouts, personal stories, expressions of annoyance and even close relationships seems to be commonplace. Even though there is potential for criminal acts to set an inappropriate example to others. According to Hootsuite (We are Social), Indonesian Digital Report 2023 Active Social Media Users are 167 million or 60.4% of the total population The Indonesian Internet Service Providers Association (APJII) survey noted that internet penetration in Indonesia has reached 78.19 percent in 2023 or penetrated 215,626,156 people out of a total population of 275,773,901 people. In observing about privacy, there are two phenomena that emerge of particular interest: on the one hand, the technological architecture of social media

pushes the boundaries of both voluntary and involuntary disclosure accompanied by privacy policies in the terms and conditions of use. (Sarikakis, K., & Winter, 2017). Social media is currently widely used as a forum for conveying information and aspirations to be used as entertainment. The process of sharing information includes not only public information but also private information. This makes many social media users share their daily lives through various available platforms such as Instagram, Twitter, Facebook, Youtube (Cahyino, 2016).

Instagram is a social media that is quite popular with its various photo and video sharing features. A few years ago, Instagram users started making second account Instagram (Sirait, 2021). This term is also known as a second account. As the name implies, the second account is an account outside the main account owned by someone. Uniquely, the second account often displays a different personality from the first account from the Instagram owner (Pramesthi, J. A., & Wulandari, 2020).

Social media users voluntarily provide personal information. When using social media, users can choose what information they want to find and be of interest to them. That is, a user can choose whether or not to be exposed to content according to what they believe and understand. This includes the attitude of users in choosing the content they want to enjoy and share (Stroud, 2014). There are various ways in which people can be selective in forming their own network and in how they choose the content they want to show and consume. CPM believes that people believe their personal information belongs to them. Because people believe they own their personal information, they also believe they have the right to control the flow of that information. Some of social media users think that personal social media with the

main account is considered a safe space for self-disclosure, so using a second account is considered to be a solution. For example, sharing locations, photos, and private outpourings. In responding to this problem, there is a need for self-communication privacy management to be able to choose information. Considering this context, it is fascinating to explore the definition of privacy among millennials and the consequences that arise when their privacy is violated. So, this is where urgency and privacy management solutions will be found in the use of social media.

Previously, there had been several studies on privacy like Scott A Wright (2019) Perceived Privacy Violation: Exploring the Malleability of Privacy Expectations, Anitha and Akash (2015) Communication Privacy Management and Self-Disclosure on Social Media - A Case of Facebook, Nick Hajli, et al (2020) Towards an Understanding of Privacy Management Architecture in Big Data: An Experimental Research, Esy Andriyani et al (Andriyani, 2019) Privacy Management of Facebook users: A study on Adolescent living in west Jakarta Slums which shows that in general young people living in slums do not understand privacy, Claire Balleys and Sami Coll (Balleys, C., & Coll, 2017) Research examines the concept of privacy for adolescents and how to experience it on social networks. Sirajul Fuad Changes in Communication Behavior of Millennial Generation and Generation Z in the Digital Age Results of research on changes in interaction patterns and understanding of millennial generation and Z generation's privacy.

From various studies, the discussion focuses more on socialization and literacy efforts, but there is research that looks at the meaning and management in the era of social media development. Therefore, this research is important to do with consideration of privacy competition in

the midst of the massive development of social media. Social media has a function and impact on people's lives, so it needs to be built in such a way that it can still fulfill these functions and goals and provide added value to everyone's life. (Fardiah et al., 2020). In addition, this research will also discuss the meaning of privacy and solutions to the problems of privacy violations that have occurred.

In addition to examining the issues at hand, researchers will utilize privacy management theory as a framework to understand and address the challenges associated with privacy violations among millennials. This theory provides a comprehensive approach to studying how individuals manage their privacy boundaries, make decisions about disclosing or concealing personal information, and cope with the consequences of privacy breaches. By applying privacy management theory, researchers can gain valuable insights into the underlying mechanisms and dynamics of privacy among millennials and develop effective strategies to mitigate the negative impacts of privacy violations. Communication privacy management theory explains that everyone has the right to their personal information. This means that someone has the ability to store or convey the information they have. Thus, personal information according to this theory is various types of information that will make a person vulnerable, therefore that person wants to control the dissemination of information that will occur in the future (Petronio, 2002, 2007, 2010, 2013). Petronio, as the originator of the theory, uses the term boundary as a metaphor which implies that there is a boundary between information that needs to be shared with others and information that is only known to oneself. (Littlejohn, 2017).

According to Petronio (2002, 2013) there are three main components

in communication privacy management theory, namely privacy ownership, privacy control, and privacy turbulence. These three components relate to how a person manages access to and protects their personal information (Petronio, 2010, 2013). First, namely privacy ownership, namely the boundaries of a person's privacy, including information that is owned but not known by others. Second, privacy control, which includes a person's decision to share personal information with other people. Petronio considers that this system is the engine of privacy management. Someone basically decides to share or disclose their personal information through certain privacy rules (Petronio, 2002, 2013). Third, privacy turbulence, which is a situation where there is an invasion of our privacy by outsiders or when privacy management does not work as expected (Petronio, 2002). In the process of managing privacy rules, Petronio (2002) divides them into three parts, namely, boundary coordination, privacy rule foundations and boundary turbulence.

There are two categories of privacy rule foundations, namely Privacy rule development and privacy rule attributes. Privacy rule development, namely the criteria for a person's decision to open or close personal information. There are five criteria in it, namely culture, gender, motivational, contextual, and risk-reward ratio (Badan Pusat Statistik, 2018). Meanwhile, privacy rule attributes consist of two supporting components, namely rule acquisition or the way people get rules and rule properties or the properties of the rules themselves. Petronio (2002) explains, boundary coordination is the process from which a person's decision is made and from which individuals are both owners of information. It consists of four main features, namely (1) boundary linkages, relationships that form boundary alliances between

individuals, (2) boundary permeability, namely the amount of information that can pass through boundaries that are made (3) boundary ownership, the process when rules determine a person's privacy boundaries and (4) boundary co-ownership, refers to the boundaries of someone who is trusted to store other people's personal information. The rules in boundary coordination do not always run smoothly, and there is a high possibility that the people involved may experience collisions or turbulence (Petronio, 2002).

Apart from using privacy management theory, this research will also use the concept of millennial generation and social media. The millennial generation is synonymous with familiarity with digital media and technology (Kaifi, B. A., Nafei, W. A., Khanfar, N. M., & Kaifi, 2012). This is one of the reasons why this study chose the millennial generation as research informants. In 2020, the year the demographic bonus starts, the millennial generation is in the age range of 20 to 40 years (Kemenpa, 2018), As already explained, if young people tend to be driven to expand their friendships, create the identity they want, and maybe even start a relationship with the opposite sex, then these circumstances can encourage someone to reveal their personal information more easily. (Petronio, 2002).

Andreas Kaplan and Michael Haenlein (Kaplan, 2010) defines social media as internet-based applications that are built and enable the exchange of user-generated content. Social media is an online platform that people use to build social networks with other people who share the same interests and activities. The background or life connection looks real. The network's impact on young people is significant. It is becoming increasingly clear that social networks have become a part of life (Akram, 2017) . Social media

also has various types and characteristics, for example YouTube which allows for audio and visuals, Instagram which is famous for its photo upload feature, TikTok which is synonymous with short videos, and Facebook which has the main strength in images and words. Therefore, the character possessed by social media will help researchers to analyze the answers of sources related to privacy violations experienced (Agung, L., & Nugraha, 2019).

The development of social media causes the meaning of privacy for each user to differ according to the level of self-disclosure they have. Social media providers should be aware that users can be worried about other users misusing their data. As our model implies, social media use is not necessarily reduced when people are worried about social risks, but it is possible that less accurate information is transmitted on both public and private social media accounts (Gruzd & Hernández-García, 2018). However, privacy on social media still needs to be managed. Experience from several cases of privacy violations which will later be studied in depth will provide an illustration of the importance of maintaining privacy on social media. The characteristics of Instagram as a social media consisting of millions of users make the relationship very complex because Instagram users come from different social classes. Yet, out of millions of highly heterogeneous users, they share similarities in the mechanisms of aesthetic production, reproduction, and consumption. The production's aesthetic is based on the principles of the genre's preferred aesthetic and this can be explored from the circle of accounts it has in common with it. Departing from various problems and theories that can be used to analyze existing cases, this research is expected to be able to answer existing problems so that in the end they can find applicable

and recommended solutions related to the urgency of privacy in the current social media era.

METHOD

This research is a qualitative descriptive research method with a constructivist paradigm. Constructivists argue that humans do not acquire or discover knowledge but construct and shape it (Denzin & Lincoln, 2009). While the research strategy used is a case study. The case study research strategy is an empirical method for investigating contemporary phenomena (cases) in depth and in real-world contexts, especially when the boundaries between phenomenon and context may not be clear (Yin, 2017). In this research, case studies are used to understand data sovereignty cases in actor networks. This stage was carried out to find out the experience of managing privacy on social media by social media users by conducting in-depth interviews with five social media users who had been victims of privacy violations using a purposive sampling technique. The informant criteria are as follows: active users of social media and aged 20-25 years. From various categorizations described by experts. In this research, the millennial generation category used is the opinion of the Ministry of Women’s Empowerment and Child Protection. In 2020, the year the demographic bonus starts, the millennial generation is in the age range of 20 years to 40 years (Kemenpa,2018). The purpose of this research includes an understanding

of privacy practices in second Instagram accounts and their impact on individuals. Therefore the use of pseudonyms or codes in research to replace the informant’s real name. This helps protect informants’ identities when referring to them in research reports. Be sure to explain why the use of pseudonyms is important to maintain the confidentiality of the informant’s identity.

In addition to add data confirmation and perspectives, the researcher also conducted interviews with two experts, namely Dr. Ikbal Maulana, National Research and Innovation Agency Researcher and Valendra Granitha Shandika Puri, M.A as a psychology lecturer. While the analysis technique used uses thematic analysis by processing the findings in the field based on the appropriate theme. Thematic analysis techniques are carried out by coding information which can produce a list of themes so that these themes can describe phenomena and help interpret the phenomena (Patton, 2002). After the research results are found, research benefits will be obtained in the form of an overview of the meaning of privacy. In addition, some of the cases that will be analyzed will provide stories about the practice of privacy violations that have occurred so as to obtain a privacy management concept that is appropriate for the millennial generation.

RESULTS AND DISCUSSIONS
Privacy Management in Second Accounts

TABLE 1. Data Research Informant

No	Informant	Gender	Age
1	Informant 1	Female	20
2	Informant 2	Female	21
3	Informant 3	Male	22
4	Informant 4	Female	22
5	Informant 5	Male	24

Currently privacy is not just personal data, but also information in a status that is uploaded in a virtual comfort zone called social media. One of the goals is self-disclosure in the form of personal stories. In the theory of communication privacy management (CPM) it is discussed about the process of individual self-disclosure initiated by Sandra Petronio. An interesting case from this CPM theory is that there are many research results related to self-disclosure in the form of privacy, individuals when disclosing their privacy, they experience anxiety when disclosing privacy either personal or group disclosure. The latest phenomenon, privacy disclosure can occur not only in person or face to face. However, self-disclosure can occur through social media by making statuses or short stories related to what individuals feel when using social media. Remember that in recent years, the explosive growth of information technology and the use of the Internet to obtain information, goods and services has sparked debate and controversy about potential threats to privacy (Singh, 2019). Privacy protection must begin to be realized and start from self-awareness. This ignorance is a result of developers' and data controllers' limited awareness and understanding, as well as a lack of tools to implement privacy by design. (Danezis et al., 2015)

It is undeniable that openness is an important factor in maintaining relationships. However, excessive self-disclosure can compromise a person's privacy or identity security. Therefore, we need to set boundaries between private information and public information (Purmiasa, S. E., Yoanita, D., & Budiana, 2020). In privacy management theory, there are three influencing elements. The first is Privacy Ownership. In the element of privacy ownership which explains that each individual feels that they are the only owner of personal information,

but when it has been disclosed to others, the information becomes shared property which has the same rights and responsibilities as well. In the context of social media, information owners have absolute control over their personal information and can independently regulate the access and diffusion of shared information. A further strong mechanism of social connection that contrasts with our fundamental demand for privacy is self-disclosure to others, which is crucial for both social engagement and psychological health. To connect with others, create lasting bonds, and obtain social support, we must be open about ourselves. Clinical signs like despair and loneliness are brought on by an inability to self-disclose (Trepte, 2011).

In using the second account, the owner has rules about who can make friends in the second account. In general, they will choose people who are considered close to be included in the second account. As stated by informant 2 who stated that he would choose someone who is open minded. The same thing was also stated by Informant 1 who considered the second account to be quite a secret room so that the selection of people who were in it was quite strict. Another reason is also related to the presence of family members on the main account, whereas according to the informant they have something that we must protect and will only share it with those they want and believe in.

Meanwhile, Informant 4 stated something different

“So the first account is for fun, the second account is for jokes. For example, on the second account you can upload any videos, yes, the term is hilarious. But for the first account, we tend to keep the “image”. In the first, the followers are family, there are certain people

who cannot be entered into the second account. Of course, it's different from the second account, whose followers are more limited because of privacy (Informant 4)."

Selection of friends who will be included in the second account is part of the privacy control. When individuals provide access to their personal information through disclosure or other means, that information enters into collective ownership, which is an extension of the boundaries of privacy. In such collective ownership, disclosure expects acceptance of responsibility for the information. As explained by Informant 4, if someone follows and doesn't meet the criteria, usually the follower request doesn't need to be accepted. Meanwhile, other informants stated that they were forced to accept but with consideration of protecting privacy by hiding stories through the hide feature. However, in terms of privacy settings, each information owner has different limits. In the strictest circumstances, the account owner may directly choose not to confirm the request. As stated by informant 5 who chose not to confirm or chose to lie if he lied if he did not have a second account.

Given that people do not consistently, effectively, or actively negotiate privacy rules to collectively retain personal information, there is a boundary turbulence. As a result, people are more likely to make someone else a co-owner of information when they have a strong connection to them. How closeness relates to rule management following a violation is less obvious. People must determine whether it is worthwhile to approach co-owners who violated private after a privacy turbulence incident. People may also decide that those ties are worth mending by confronting the co-owner about the improper handling

of their personal information because they are more likely to wish to disclose to those who are dear to them (Steuber & McLaren, 2015). Limit turbulence occurs when unintended violations, interruptions or mistakes are made in such a way that co-owners control and regulate the flow of personal information to third parties. In using the second account itself, the owner has experienced a violation. As stated by informant 4 who had experienced a violation in the form of spreading photos that were uploaded to the second account and then given to the group without confirmation. Based on this statement, it is known that the second account is considered a safe zone and a place that is quite trusted but does not rule out the possibility of privacy violations. Many issues can arise from the sharing of private information, and as a result, this can cause consumers to get anxious as they consider whether to share this information or not, and, in the end, to experience delays in the process of expressing their opinions (Pelteret & Ophoff, 2016). Even the culprit was a well-known figure. The same thing was also experienced by informant 3

"There was a time when I was doing something, then in the second I also took lots of my photos which were scattered everywhere because they were captured. Finally, I tried to find the person, I found it and finally I deleted it. Turns out he caught the other meaning that's why he said it here and there. (Informant 3)"

This shows that the ownership of information cannot be addressed properly. It is undeniable that on social media someone feels they have information and there are no clear rules. Informant 2 had different experiences

"We have close friends. I was close

to him, at first he talked about going to college for a long time, uh, you have a girlfriend. Looks like we broke up with that. So it's like when everyone is dating, we are perfectly single together. Well, sometimes he forgets about me. He plays with other friends. So arrogant. When I entered college, he didn't look at the campus at all.. Really don't even look at it. Keep posting likes (Forgot friends). Until he unfollowed my second account. (Informant 2)"

Based on these data, it can be seen that information rules that are considered privacy are faced with a dilemma. The concepts of secrecy and privacy have overlapping, muddled connotations. People can observe formal or informal organizational artifacts and actions that convey both visible and unseen attitudes and ideas regarding whether information should be disclosed or kept private (Bean, 2017). Everyone has a different definition of privacy, so what is meant as privacy for one person may not necessarily apply to another person. Information privacy is primarily concerned with the protection of personally identifiable information. Information privacy is an uphill task, particularly, in the adaptive context of complex and multi-stakeholder heterogeneous digital ecosystems (Anwar, M. J., Gill, A. Q., & Beydoun, 2018). Therefore, the meaning of each individual's privacy needs to be determined so that meaning bias does not occur and privacy can be managed more wisely.

Privacy Management and Second Account as a Place for Self-Disclosure

Privacy management is one of the key issues amid the development of social media. Security of data and trust related

to information seems to be absolutely necessary. Second account is considered as a safe place to disclose stories that are considered private. People have the option to express themselves more freely or anonymously with a second account. Users may share personal information for purposes other than their primary account for a variety of reasons. The desire for privacy is underappreciated in part due to the fact that people's activities to defend their private are so common and natural that they are ignored or are not recognized as privacy behaviors. (Krishna, 2020). Setting limits for what is shared or kept private on the second account is part of privacy management. Users have the option to use aliases, use a new profile photo, or manage who gets access to their secondary account. They can modify privacy settings to restrict who sees their postings and personal data. Second account users basically choose to open their privacy even though they still have the option not to upload because social media has become a place for fun, as stated by informant 1

"Yes, young people want to capture moments, right? Capturing the moment like I have a boyfriend now. For example, something is funny. It's a shame if it's not told. What's it like? It's only in the gallery. It's like holding back from posting a story when the story person isn't strong either. (Informant 1)"

But social media comes with a sense of satisfaction. Regardless of culture and gender, there is a mediated negative relationship between social media addiction and life satisfaction (Hawi, N. S., & Samaha, 2017). This is reflected in the user's desire to capture moments with social media, which often blurs privacy boundaries. As explained by informant 4 who used a second account to capture the

moment and felt that he was well known by close friends. Meanwhile, informant 5 said that the second account is a container for sharing private information that you want to open

“Because there is privacy that can still be shared. Usually photos in feeds anyway The frequency at first is weird. (Informant 5).”

Based on these various statements, the informants basically realized that there was a threat of privacy violations on social media. The way of conveying information generally starts from general things and then indents on special things. The ease of conveying information is increasingly felt if there are similarities between the two communicators, the delivery is interesting and touches one's emotional side (Hermawati, T., Setyaningsih, R., & Nugraha, 2021). One of the goals underlying this is the desire for self-disclosure. Self disclosure is also interpreted as relationship management. The theory of communication management or communication management is motivated by the tendency of social media users to visit each other's pages with other users (Cahyaning, A., & Cahyono, 2015).

The phrase “privacy management” describes people's efforts to regulate and keep track of the private information they disclose to others. Because users frequently utilize the second account as a location for self-disclosure that is more free-form or anonymous, privacy control on Instagram becomes crucial in this context.

“Because, the individual that shared by someone in the second account, feel belong to the group. This feeling of affiliated to such group correlated with Maslow's Theory of Needs. Besides, the

personal ego such as appreciated by other or trusted by someone in second account also is the part of individual Esteem Needs based on Maslow's theory (Valendra Granitha Shandika Puri, M.A, Psychology lecturer)”

Users of the secondary account could provide personal information for distinct reasons not present in their primary account. They could want to keep their identities partially hidden in the main account in order to safeguard their privacy. This may be related to the desire to integrate personal and professional lives, to retain privacy from those closest to them, or to explore other facets of oneself without disclosing one's genuine identity. Setting boundaries on what you wish to reveal or keep secret in a second account is an example of privacy management in this situation. Users have the option to use a false name, select a different profile picture, or manage who gets access to their second account. To restrict who can see their postings and personal information, they can also select privacy settings.

The process of dissemination of information through second accounts can be carried out accidentally or as the result of the desired search. A popular term that describes visits between social media account owners is known as a stalker (Arslan, N., & Kiper, 2018). Not infrequently through stalker activities someone will have an assessment of other users (Njotorharjo, 2014). It is from this variety of curiosity that can potentially lead to various perceptions regarding the information obtained. So it is not uncommon for this information to be disseminated again to third parties with various motives.

Through this phenomenon, it can be said that self-disclosure on social media is an unavoidable motive. Self-disclosure

is the ability of individuals to provide responses, reactions and information about themselves that they usually hide from other people or the process of individuals in establishing relationships to become closer to others. (Aziizatun Nabillah, N., & Hanurawan, 2022). By using the close friend feature, users feel that their way of expressing themselves can be freer and safer, but in reality data breaches are still a threat and even lead to divisions in friendships. Relationships with others depend on openness and discretion. While telling another person what you're going through can be beneficial for your relationship and for yourself, crossing private lines can also be risky (though it might also be gratifying) (Kennedy-Lightsey et al., 2012). Even though nothing is safe in social media because there is still the potential for hacking

“The protection of user data from hacking attempts is a fundamental pillar of the social media business model, and social media platforms prioritize maintaining a reputation as providers of reliable security measures. Their utmost priority is to have exclusive access to user data. While they facilitate targeted advertising to reach the right customers, they ensure that advertisers do not have direct access to the data themselves. However, the security measures cannot provide foolproof protection for all users. Some novice users opt for easily guessable passwords, which can be exploited by unauthorized individuals, leaving them vulnerable to potential security breaches.. (Dr. Iqbal Maulana, National Research and Innovation Agency Researcher)”

Users have different boundaries

regarding the privacy they disclose on Instagram (Agung, P., & Arofah, 2012). In addition, they have different ways of disclosing their privacy. In addition, the audience analyzed takes into account the risks and benefits they will experience when making disclosures via Instagram (Sakinah, 2021). The dimensions of self-disclosure can be seen from size, valence, accuracy & honesty, intent & purpose, and depth. Each informant has a different statement. How much time is needed for individual self-disclosure on social media will influence other individuals to understand themselves in their uploads (Siregar, 2022). Therefore, in an effort to manage privacy on social media, especially in the use of the close friend feature on Instagram, it is important to be wiser in publishing information, especially those that are considered private or even curses of annoyance to vent that feel safe (Finaka, 2018). Even though in reality it still has the potential to be received by parties who should not get this personal information. It should be remembered that if information has been disseminated through social media, the ownership of information will become more biased and unpredictable. Organised disinformation operations may also be aided by technological developments which will increasingly facilitate large-scale automated generation and dissemination of disinformation content (Botero Arcila & Griffin, 2023)

The second account phenomenon signifies Instagram as an emotional vessel for owners to express various self-expressions. To upload content on Instagram, someone usually has several considerations (Natalia, 2018). Through their second account, a person usually expresses various expressions ranging from happiness, sadness, anger to disappointment in a deeper way. The second account usually functions differently from the first account where

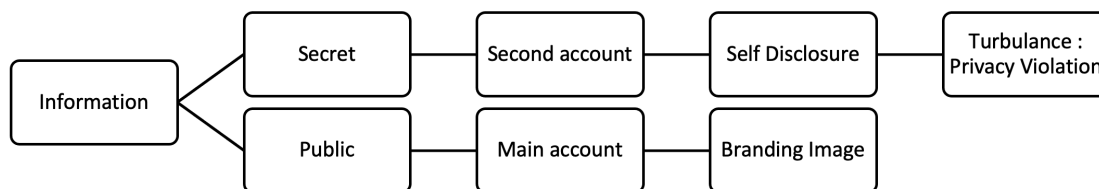


FIGURE 1. The Pattern of Privacy Main Account Vs Second Account

the second account can be used as a ‘safe space’ or a place for self-performance (Paramesti, A. R., & Nurdiarti, 2022). In general, the second account phenomenon in the context of privacy in the millennial generation can be described in the Figure 1.

Based on this pattern, it can be seen if the use of a second account is adjusted to the category of public or confidential information. From a usage standpoint, the second account will focus on freer self-disclosure, while the main account has some limitations set by the account owner himself so that it tends to lead to branding image. With this rule, the potential for turbulence is more on the second account because the people in it are those who are already trusted so that if information is leaked, there will be violations that lead to suspicion and disputes.

Freedom of expression on social media sometimes makes users not think twice about uploading content. This privacy management is getting worse in some teenagers who do not have mature self-control (Anggara, 2021). In the theory of communication privacy management, a person has the right to disseminate information about himself so that he will create boundaries in sharing it with others (Ardiyanti, 2018). This means that the management of privacy owned by one individual to another individual will certainly be different. Privacy is something that is limited so that other people may not necessarily know it (Bazarova, 2014). In the era of modernization, the speed of information delivery and the flexibility of social media

must be balanced by maintaining ethics in social media. Utilization of the sharing feature is not only interpreted as spreading information but as protection of personal data (Ramirez, F. A., & Lane, 2019). After all, the development of healthy, safe and comfortable media activities depends on digital ethics. These contacts often trigger irresponsible comments on their social media (Pramesti, 2023).

CONCLUSION

Managing privacy on social media is absolutely necessary. Social media users are often faced with the choice of storing information in its entirety or partially opening it through a second account. However, the threat of privacy violations can also occur in the second account and even lead to splits in friendship. Conveying information generally starts from general matters and then indents to specific matters, both consciously and unconsciously. The various violations that occurred on the second account were caused by a lack of knowledge and a misguided understanding that data would be stored safely with the closest trusted person. Even though the person who is selected to enter the second account circle is also vulnerable to opening the account owner’s private data and even spreading it. In an effort to manage privacy on social media, especially in the use of the close friend feature on Instagram, it is important to be wiser in publishing information, especially those that are considered private or even curses of annoyance to statements that are felt to be safe. This is where the urgency of

privacy management is needed. The ease of conveying information and the desire for various social media stories must be balanced by maintaining ethics in social media. Therefore, through this paper the researcher provides recommendations to various parties. First, social media users should have clear rules regarding the meaning of privacy by considering the urgency and potential for violations that may occur. Second, the government should consistently socialize regulations related to violations of personal data and the urgency regarding data protection. The next research is expected to be able to further examine prevention and therapy strategies for social media users who are already addicted so they cannot manage their privacy.

REFERENCES

- Agung, L., & Nugraha, N. D. (2019). Digital Culture and Instagram: Aesthetics for All? Universitas Multimedia Nusantara. <https://doi.org/Digital Culture and Instagram: Aesthetics for All?>
- Agung, P., & Arofah, K. (2012). Media sosial instagram sebagai sarana sosialisasi kebijakan penyiaran digital. *Jurnal Komunikasi*, 2, 256–269.
- Akram, W. dan R. K. (2017). A Study on Positive and Negative Effects of Social Media on Society. *International Journal of Computer Sciences and Engineering*, 5.
- Andriyani, J. (2019). Strategi Coping Stres Dalam Mengatasi Problema Psikologis. *At-Taujih : Bimbingan Dan Konseling Islam*, 2(2), 37. <https://doi.org/10.22373/taujih.v2i2.6527>
- Anwar, M. J., Gill, A. Q., & Beydoun, G. (2018). A review of information privacy laws and standards for secure digital ecosystems.
- Arslan, N., & Kiper, A. (2018a). Self-Disclosure and Internet Addiction. In *Malaysian Online Journal of Educational Technology* (Vol. 6, Issue 1). www.mojet.net
- Asosiasi Penyelenggara Jasa Internet Indonesia. (2023). *Info Grafis Penetrasi dan Perilaku Pengguna Internet di Indonesia*.
- Azizatul Nabillah, N., & Hanurawan, F. (2022). Association Between Self-esteem and Self-disclosure in Female University Students as Second Instagram Account Users in Malang. *KnE Social Sciences*. <https://doi.org/https://doi.org/10.18502/kss.v7i18.12393>
- Badan Pusat Statistik. (2018). *Statistik Gender Tematik: Profil Generasi Milenial Indonesia*. Kementerian Pemberdayaan Perempuan dan Perlindungan Anak dan Badan Pusat Statistik.
- Balleys, C., & Coll, S. (2017). Being publicly intimate: teenagers managing online privacy. *Media, Culture and Society*, 39(6), 885–901.
- Bean, H. (2017). Privacy and Secrecy. In *The International Encyclopedia of Organizational Communication* (pp. 1–14). Wiley. <https://doi.org/10.1002/9781118955567.wbieoc170>
- Botero Arcila, B., & Griffin, R. (2023). Social media platforms and challenges for democracy, rule of law and fundamental rights Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 743.400-April 2023 En Study.
- Cahyaning, A., & Cahyono, T. R. (2015). Perbedaan Communication Privacy Management di Media Sosial Twitter pada Remaja dengan Tipe Kepribadian Extravert dan Introvert. *Jurnal Psikologi Pendidikan Dan Perkembangan*, 4(1).
- Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R., & Schiffner, S. (2015). Privacy and Data Protection by Design - from policy to engineering. <https://doi.org/10.2824/38623>
- Denzin & Lincoln. (2009). *Handbook of Qualitative Research*. Pustaka Pelajar.
- Fardiah, D., Rinawati, R., Darmawan, F., Abdul, R., & Lucky, K. (2020). *Media Literacy For Dissemination Anticipated*

- Fake News On Social Media. *Mediator: Jurnal Komunikasi*, 13(2), 278–289. <https://doi.org/10.29313/mediator.v13i2.6624>
- Gruzd, A., & Hernández-García, Á. (2018). Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media. *Cyberpsychology, Behavior, and Social Networking*, 21(7), 418–428. <https://doi.org/10.1089/cyber.2017.0709>
- Hawi, N. S., & Samaha, M. (2017). The Relations Among Social Media Addiction, Self-Esteem, and Life Satisfaction in University Students. *Social Science Computer Review*, 35(5). <https://doi.org/576-586>. <https://doi.org/10.1177/0894439316660340>
- Hermawati, T., Setyaningsih, R., & Nugraha, R. P. (2021). Teen Motivation to Create Fake Identity Account on Instagram Social Media. *International Journal of Multicultural and Multireligious Understanding*, 8(4). <https://doi.org/https://doi.org/10.18415/ijmmu.v8i4.2459>
- Kaifi, B. A., Nafei, W. A., Khanfar, N. M., & Kaifi, M. M. (2012). A multi-generational workforce: managing and understanding millennials. *International Journal of Business & Management*, 7(24), 88–93.
- Kaplan, A. and M. H. (2010). Users of the world unite! The Challenges and opportunities of social media. *Business Horizons*, 53(1), 59–68.
- Kennedy-Lightsey, C. D., Martin, M. M., Thompson, M., Himes, K. L., & Clingerman, B. Z. (2012). Communication Privacy Management Theory: Exploring Coordination and Ownership Between Friends. *Communication Quarterly*, 60(5), 665–680. <https://doi.org/10.1080/01463373.2012.725004>
- Krishna, A. (2020). Privacy is a Concern: An Introduction to the Dialogue on Privacy. *Journal of Consumer Psychology*, 30(4), 733–735. <https://doi.org/10.1002/jcpy.1186>
- Koidl, K., Conlan, O., Reijers, W., Farrell, M., & Hoover, M. (2018). The bigfoot initiative: An investigation of digital footprint awareness in social media. *ACM International Conference Proceeding Series*, 120–127. <https://doi.org/10.1145/3217804.3217904>
- Littlejohn, S. W. (2017). *Theories of Human Communication 11th Edition*. USA: Waveland Press.
- Miles, M. B., Huberman, A. M., & Saldana, J. (2013). *Qualitative data analysis: A methods sourcebook*. London: Sage Publications.
- Paramesti, A. R., & Nurdiarti, R. P. (2022). Penggunaan Pseudonym di Second Account Instagram dalam Perspektif Etika Digital. *Jurnal Communio: Jurnal Ilmu Komunikasi*, 11(1).
- Patton, M. Q. (2002). *Nontraditional Regulations, and Innovations in Darning-Centered, Doctoral Education, Including Faculty Meetings That Are Interesting and Important, an Indication of Knovation of the Highest Order In Qualitative Inquir*.
- Pelteret, M., & Ophoff, J. (2016). A Review of Information Privacy and Its Importance to Consumers and Organizations. In *Informing Science: the International Journal of an Emerging Transdiscipline (Vol.19)*. <http://www.informingscience.org/Publications/3573>
- Pramesthi, J. A., & Wulandari, E. (2020). Communication Privacy Management: Studi Literatur Pada Batasan Privasi Dalam Konteks Keluarga Indonesia. *Jurnal Ranah Komunikasi (JRK)*, 4(2). <https://doi.org/https://doi.org/10.25077/rk.4.2.122-132.2020>
- Pramesti, O. L. (2023). Penerapan Etika Digital di Kalangan Content Creator TikTok. *Mediator: Jurnal Komunikasi*, 15(2), 236–248. <https://doi.org/10.29313/mediator.v15i2.10460>
- Purmiasa, S. E., Yoanita, D., & Budiana, D. (2020). Factors of Public Self-Disclosure Via Instagram Stories.
- Ramirez, F. A., & Lane, J. (2019). Communication Privacy Management and Digital Evidence in an Intimate Partner Violence Case. *International Journal of Communication*, 13.
- Roessler, B., & Mokrosinska, D. (2013). Privacy and social interaction.

- Philosophy and Social Critism, 39(8), 771–791.
- Saidah, M. (2019). Kebebasan berekspresi dan paradoks privasi dalam hubungan pertemanan. 3(2).
- Sakinah, S. (2021). Analysis of the Use of Close Friend Feature on Instagram as a Social Networking Site Using Communication Privacy Management Theory. *Jurnal Pewarta Indonesia*, 3(2), 95–104. <https://doi.org/https://doi.org/10.25008/jpi.v3i2.85>
- Sarikakis, K., & Winter, L. (2017). Social Media Users' Legal Consciousness About Privacy. 3(1). <https://doi.org/>. <https://doi.org/10.1177/2056305117695325>
- Singh, D. (2019). Ethical Dilemmas on Data Privacy and Security for Social Media's Users. *SSRN Electronic Journal*. <https://doi.org/https://doi.org/10.2139/ssrn.3395616>
- Sirait, A. R. (n.d.). Spectatorial Sisterhood: Relasi Sosial Pengguna Second Account di Instagram (Vol. 42, Issue 1). <https://instagram-press.com/>.
- Sirait, A. R. (2021). Spectatorial Sisterhood: Relasi Sosial Pengguna Second Account di Instagram. 42.
- Siregar, A. H. (2022). Privacy Anxiety on Micro-Influencers in Self-Disclosure through the Add Yours on Instagram Social Media. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, 5(3).
- Steuber, K. R., & McLaren, R. M. (2015). Privacy Recalibration in Personal Relationships: Rule Usage Before and After an Incident of Privacy Turbulence. *Communication Quarterly*, 63(3), 345–364. <https://doi.org/10.1080/01463373.2015.1039717>
- Trepte and Reinecke. (2011). In *Privacy Online*. Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-642-21521-6>
- Wahyu Natalia, I. (n.d.). *Communication Privacy Management (Manajemen Komunikasi Privasi) tentang Hubungan Seks Pranikah yang telah dilakukan oleh Remaja*. www.kaskus.co.id
- Yin, R. K. (2017). *Case Study Research and Applications*. <https://doi.org/http://ir.obihiro.ac.jp/dspace/handle/10322/3933>