Jurnal Pewarta Indonesia
Volume 3 No 2 – 2021, page 95-104
Available online at http://pewarta.org

Analysis of the Use of *Close Friend* Feature on Instagram *as a Social Networking Site* Using *Communication Privacy Management* Theory

Sofa Sakinah
Department of Communication, Universitas Indonesia
Jl. Salemba Raya No. 4, IASTH Building Lt. 6. Jakarta 10430 – Indonesia
Corresponding author: sofa.sakinah@ui.ac.id

DOI: http://dx.doi.org/10.25008/jpi.v3i2.85
Submitted: 15 Agustus 2021 **Revised**: 16 Oktober 2021 **Published**: 31 Oktober 2021

Abstract - The development of digital media technology gave rise to social media, especially Instagram which is a site used to exchange information and fulfill social communication needs in various circles. This study specifically analyzes the use of the *Close Friend* feature found on Instagram social media which is used for various objectives of each user. The research method uses descriptive quantitative content analysis through text analysis from various previous studies related to the use of the Instagram feature. One study showed that the effectiveness of the Instagram feature in increasing adolescent friendships in the digital era was dominant in the *Close Friends* feature as much as 61.2%. Close friends feature (*close friend*) was promoted because of the self-disclosure factor, as well as the convenience of users in uploading Instagram stories. The level of openness to the high categorydue to the proximity selecting and *content sharing* on this feature. The close friends feature is considered more *private* for Instagram users because they are free to choose their audience and upload based on their needs and desires. It was also mentioned how users manage their privacy when using the Instastory feature on Instagram social media where the privacy management is based on the *Communication Privacy Management* (CPM) criteria or *Communication Privacy Management* and is seen in the usage strategy when using the Insta Story feature on Instagram. Informants tend to have different reasons behind their decision to reset their privacy when using their social media.

Keywords: Social Networking Site, Instagram, Communication Privacy Management

Introduction

New media, also known as digital media, are media whose content has a combined form of data, text, sound and various image content that is stored in digital format which is then disseminated using *broadband* optical cable-based *networks*, satellites and microwave transmission systems (Flew, 2008). According to McQuail (2010), digital media has a focus on interconnection between users, where each user is referred to as *senders* and *receivers*. Digital media is categorized as a form with no clear head of protection. The existence of freedom of access to content viewed by users may lead to abuse which may cause widespread fear. McQuail emphasized that with the emergence of digital media which is a new media, media analysts have conducted a review of studies on the effects of the media itself. They consider that this form of unidirectional mass communication is no longer appropriate to continue to be used in the future. Digital media itself is a closed institution which is quite difficult to regulate the communication pattern. The principle of digital media is practically the same as mass media, which basically means that the communication process is available to everyone.

Social Media is a medium that users can connect, share, and then form social networks in cyberspace. The development of blogs and also various social networking platforms is a form of social media that can be accessed very easily by various media users in the world. Andreas Kaplan and Michael Haenlein (2010) make a definition of social media. They say that social media is an internet-based network and is built on the basis of the development of website technology. This allows *user-generated content to* occur.

The development of digital technology and the internet that is increasingly advanced makes the development of social media also grow rapidly. Currently, accessing various social media applications can be done anywhere and anytime using only a *smartphone*. The speed in accessing information through social media can make various major phenomena such as mass movements demand something. This happens in both developed and developing countries such as Indonesia. With the speed of access to information, social media has also begun to reduce the popularity of conventional mass media in terms of the dissemination of actual news (Lesmana, 2012).

The most common definition of *Social Networking Sites* (SNSs) is that proposed by Boyd & Ellison (2008, p. 211) which defines SNSs as web-based services that enable individuals to: (1) have a public or semi-public profile account in an involved system; (2) show a list of other users with whom or with what accounts they share the connection, and (3) view and track a list of each user's connections and/or those made by other users in a system.

Cornelissen (2014) also explains that social networking sites allow users to find new friends and even expand their circle of friends that are not just friends in real life (Cornelissen, 2014). In addition, another word for SNSs, namely *Online Social Networks* (OSN) (Kayes & Iamnitchi, 2017) is a permanent presence in the personal and professional life of today of a large segment of the population, with direct consequences for offline activities. Built on a foundation of trust - users connect to other users with similar interests or overlapping personal trajectories - OSN and related applications extract unprecedented volumes of personal information. *Online Social Networks* (OSN) have become a major cultural phenomenon for millions of Internet users by combining user-generating profiles with communication mechanisms that allow users to become pseudo-permanently "in touch", increase users' real-world social connections and better integrate our online and offline lives. Not surprisingly, then, serious privacy and security risks arise, positioning themselves along two main types of attacks: attacks that exploit implicit trust embedded in stated social relationships; and attacks that harvest users' personal information for unwanted use (Kayes & Iamnitchi, 2017)

Instagram as SNS and the Close Friend Feature

Instagram is one of the social media that has very many users, which has the main service for sharing photos and videos. It was explained that Instagram social media users in Indonesia in November 2019 reached 61.6 million users (Kompas.com, 2019). Instagram has many users because of the advantages it has, such as a means of exchanging or providing information, the features that are used for business development, the ease of using the service, to the freedom to use an Instagram *account* to present products or as a media portfolio of works (Dewi & Janitra, 2018).

Another interesting factor from Instagram social media is analyzing how users interact and treat their accounts very varied. Sherry Turkle in (Dewi & Janitra, 2018) explained that networked technology makes a person have a more fluid and fragmented identity. In their writings, Palfrey and Gaser explain that the birth of the internet has also led to changes in the *mean* or meaning in an effort to build and manage identity while in the online world.

Many Instagram fans now have more than one Instagram account or even limit the audience that can reach their uploads. One study revealed that Instagram users use other accounts to show the self-image that the account owner wants to build to their target audience, while other accounts are used by the owner to upload things that reflect their different characters (Kang & Wei, 2018). Account users do not want to show themselves in *real* because their main account is used to show their positive image (Dewi & Janitra, 2018), can be accessed by many people (Emeraldien, Aulia, & Khelsea, 2019) and has the potential to create controversy or offend a parties (Kang & Wei, 2018).

In 2018, Instagram released a close friend feature that allows users to select who can access the uploads published by the owner. These points are intended to provide comfort for Instagram users when explaining things that are of course intended for the people around them that they want (Pardes, 2018).

There is something that is quite interesting that some people continue to use the services of close friends on their other accounts in which there is a close audience and an audience that the account owner has trusted. This fact contributed to the existence of this research. The research conducted is also used to find out what the actual objective of the account owner is to use the close friends feature and how the communication privacy management process they do.

Closest friends are emotional relationships that grow between two or more individuals, both of the same sex and of different genders, which are based on mutual understanding, respect, and trust between one another (Diantika, 2017). Close friends have an influence on the formation of individual character or personality. In many cases, close friends have a strong enough impact in making big decisions (Zulfa, Heryaniningsih, Saputra, & Putri, 2018). Close friends can be the center of social and emotional support, because friends have the function of providing ego support, intimacy or attention, and making individuals able to express their identities properly and appropriately (Rahma & Prasetyaningrum, 2015).

Social networking can be said to be a very popular thing in today's world as it can be seen that millions of people have used various forms of social networks that allow individuals to connect with friends and family, and share personal information. However, problems related to maintaining the privacy and security of a user's information can occur, especially when the content uploaded by the user is multimedia, such as photos, videos, and audio (Rathore et al., 2017).

The emergence of choices regarding the appearance of public connections is used as a crucial factor in SNS. The friends list includes links to each friend's account, which makes it possible for other users to browse the network by clicking on the friend account list. On most sites, the friends list is visible to anyone who is allowed to view the profile, although there are exceptions (Boyd & Ellison, 2008).

Theoretical Frameworks

The Communication Privacy Management theory, coined by Sandra Petronio, is presented to explore the privacy management system that is run by individuals in managing their personal information. Petronio said that communication privacy management theory provides a mind map that describes a system for understanding the communicative aspects of how people make judgments about the management of their personal information with others (Petronio, Communication Privacy Management Theory, 2016).

Petronio has an assumption that the exposure of personal information can lead to two different directions (Griffin, 2011). The first option is that the disclosure of personal information can be a step in strengthening the relationship between the original owner of the information and the recipient of the information. The second thing that makes it possible is that the disclosure of personal information can also lead to a messy relationship when the other party turns out to be unable to deal with what is conveyed to the individual, it could even be that the person intentionally shares the information with others. In 2013, Petronio explained that there were three prominent axioms in CPM theory, namely privacy ownership, privacy control, and privacy turbulence (Petronio, Brief Status Report on Communication Privacy Management Theory, 2013).

Thompson describes three crucial principles in CPM Theory, namely (Thompson, Petronio, & Braithwaite, 2012):

(1) Privacy ownership means that individuals believe that they are the real owners of their personal information. They have the right to decide whether to give or deny access to their personal information and determine how the recipient of the information should behave with that information (Petronio, Communication Privacy Management Theory, 2016);

(2) Privacy control is an activity where the original owner of the information makes rules regarding matters relating to his personal information. In addition, when providing such information, the original owner expects the recipient to comply with the previously established rules. There are three limitations that need to be discussed by the owner with the information, namely boundary ownership,

boundary linkage, and boundary permeability (Griffin, 2011). *Boundary ownership* relates to ownership of information and who decides whether or not personal information is shared with third parties. Boundary linkage relates to parties who are allowed to know the personal information. Boundary permeability relates to how much personal information can be shared with third parties;

(3) Privacy turbulence occurs when the co-owner of the information does not know or does not comply with pre-established rules. Privacy turbulence can cause disruption to complete failure of existing privacy management.

Griffin also divides privacy turbulence into 3 (three) categories, namely fuzzy boundaries, intentional breaches, and mistakes (Griffin, 2011). Fuzzy boundaries are situations when the co-owner of information does not have any negotiation or agreement regarding information *boundaries* that can be presented. *Intentional breaches* are conditions where the co-owner knows the existing agreement, but deliberately disobeys the agreement. Meanwhile, mistakes are situations where the co-owner of the information spreads the personal information unintentionally.

Communication Privacy Management (CPM) is a theory that describes a map that shows that people make choices about disclosing or hiding private information based on criteria and conditions that they consider important, and individuals believe that they have the right to own and regulate access to their private information (Petronio, 2002). Communication Privacy Management (CPM) is interested in explaining people's negotiation processes around disclosing private information. "*CPM theory offers a privacy management system that identifies ways privacy boundaries are coordinated between and among individuals*" (Petronio, 2002).

Communication Privacy Management Theory from Sandra Petronio, communicators should have their own judgment and choice of regulations regarding what to say, and what to keep from the public. We must consider and organize the messages we produce, share and distribute to a wide audience.

If you see many cases of someone's unwiseness in social media, it is not caused by low or high education but is related to the mentality of the user. Some case examples show that the potential can be experienced by anyone who uses social media beyond legal and ethical boundaries.

For example, the strangeness of the title and content, the lack of clarity of the source, the ambiguity of the media *links* it uses, which are sensational and often provocative, and a number of other markers. However, hoaxes are often easily accepted by people because they are often good at taking advantage of the psychology of people who are hit by comfort, uncertainty, disappointment, so they often ignore the limits of communication privacy that should be maintained and managed.

Basic Assumptions of Communication Privacy Management

Communication Privacy Management Theory (CPM) is interested in explaining people's negotiating processes around disclosing private information. Petronio (2002) states that people define private information as information about things that are very meaningful to them. Therefore, the process of communicating private information in relation to other people becomes private disclosure. CPM focuses on self-disclosure rather than self-disclosure. This emphasis away from self-disclosure makes a clear distinction between the definition of CPM and traditional research on openness. CPM views this definition differently in three ways. First, self-disclosure places more emphasis on the personal content of disclosures than traditional literature on self-disclosure. In addition, CPM studies how people do disclosures through a system based on rules, and lastly CPM does not see that disclosure is only related to self. As Petronio (2002) observes, this CPM theory does not limit this process to the self, but extends to include many levels of opening including the self and the group.

Communication Privacy Management Theory proposes five basic assumptions: private information, private boundaries, control and ownership, a rule-based management system, and management dialectic. The first assumption is Private

Information, Petronio defines private information as information about things that are very meaningful to them, "what makes something private is how important it is to our conception of ourselves and to our relationships with others".

Therefore, there are two concepts in this private information, namely intimacy and personal disclosure (West & Turner, 2008). The second assumption is Private Boundaries, on the assumption that there is a "boundary line" that provides a boundary between being public and being private. On one side of this limitation, a person will keep private information for himself (Giles, Gallois, & Elemers, 1998) and on the other hand people will disclose some private information to others in their social relationship with them. When private information is shared within the boundaries around it, it is called a *collective boundary*, whereas when private information chooses to be kept by an individual and not disclosed to anyone, the boundary is called a *personal boundary*.

The third assumption is Control and Ownership, this assumption explains that everyone who feels they have private information about themselves, they believe that they should be able to control who (if any) is allowed to access this information. The fourth assumption is a Rule-Based Management System, which explains that this system is a framework for understanding the decisions a person makes regarding private information. Rules-based management systems allow processing at individual and collective levels and are complex arrangements consisting of three processes: privacy rule characteristics, boundary coordination, and boundary turbulence.

The characteristics of privacy rules have decision criteria, namely cultural, gender, motivational, contextual, and risk-benefit ratio. Boundary coordination refers to how individuals manage shared information with co-owners of private information. Then boundary turbulence relates to situations where the rules on boundary coordination are not clear, or one of the parties violates them. Finally, the fifth assumption is Management Dialectic, this assumption focuses on the tensions between the desire to disclose private information and the desire to cover it up.

The roots of the theory of Communication Privacy Management (CPM) theory are assumptions about the way an individual thinks and communicates. The definition of information in this theory is something secret (private), which means that the information is very meaningful to them or it can also be called private information (Sarafinelli, 2019).

It is this ability to manage private information that makes people feel that they are the rightful owners of the information shared about themselves. So, they have the right to set boundaries for others. Privacy rules have five characteristics, namely based on cultural criteria, gender criteria, motivation criteria, context criteria and risk and benefit ratio criteria. (West & Turner, 2008:261). These principles are basically how to define self-disclosure made on Instagram set through the disclosure of privacy information. So that Instagram users need to set controls and limits when disclosing information in order to protect their personal information (Liu, Z., & Wang, X. 2018).

Material and Methodology

Privacy Management on the use of social media can happen to everyone who uses the channel to communicate. The method used in this research is a qualitative approach. While this type of research uses a qualitative descriptive type. Where the researcher will explain how Instagram platform users manage their privacy when using the *close friend* feature for various purposes.

Methodology The research approach that will be used is a qualitative approach. Qualitative researchers emphasize the socially constructed nature of reality, besides that there is a close relationship between the researcher, the subject, and the pressure of the situation (Nugrahani, 2014). To get information is done by collecting data themselves through checking documents, or observing behavior (Creswell, 2009:175).

Qualitative research has a tendency to collect, analyze, and interpret data simultaneously. Data collection is done by collecting data through literature studies. Literature study is a method that collects theory and research related to research topics

(Ridley in Mizanie & Irwansyah, 2019). All literature searched and collected came from various sources such as books, journals, news, and the results of previous research. After all the literature is collected, then the research is carried out by compiling the literature according to the topic so that it can provide broader conceptual knowledge.

Result and Discussion

In CPM theory, information is very meaningful to individuals or it can also be called private information. It is this ability to manage private information that makes people feel that they are the rightful owners of the information shared about themselves. So, they have the right to set boundaries for others. Privacy rules have five characteristics, namely based on cultural criteria, gender criteria, motivation criteria, context criteria and risk and benefit ratio criteria. (West & Turner, 2008:261).

Based on the latest research conducted by Zainuri in 2021 regarding the use of the Close Friend feature on Instagram used by students at Sebelas Maret University, it can be concluded that in general, informants claimed to use the close friend service on their second account because they felt uncomfortable and wanted to keep their privacy. In addition, informants use the close friend service to provide information that they think is dangerous if shared with the wider public. Informants also use the close friend service on the second account to avoid wrong judgments when sharing something on their second account in general. In addition, the informant also uses the close friend service on his second account because he needs space to issue his complaint (Zainuri, 2021).

In determining who is allowed to know the personal information they share, each informant has their own way. This is because the account followers of the two informants are already their close friends, so another, more personal reason is needed. Some have three categories of considerations, based on emotional closeness, people who are more trusted than others, and have similar interests.

In determining the private limits regarding their personal information, seven out of eight informants admitted that they did not negotiate the existing limits with the people they put on their close friends list on their second account. This is because the account owner has given trust and hopes that the people they enter will understand by themselves that the information shared is personal information.

Meanwhile, one informant admitted to conveying the limitations he had because he thought that everyone had a different way of managing their own close friends.

In conditions of privacy turbulence, each informant deals with it in a different way. Some of the informants responded based on the impact they had, talking directly to the person spreading the information, or choosing to keep their distance. Regarding the action to be taken, most of the informants admitted that they would remove the person from the close friend list of their second account. Meanwhile, several informants claimed to be removing the person from their second account, blocking the person, or choosing not to take action.

Another study conducted by Kamilah and Lestari in 2020 revealed that users use Instagram to create an impression, interest, relationship and build the image of Kamilah & Lestari, 2020). In addition, users also have different information boundaries regarding their privacy. Through the *Communication Privacy Management* theory, it was also stated that there are regulatory criteria used by users to consider when they want to disclose information through Instagram. Cultural criteria such as customs, norms, and religious values that exist in users, gender criteria in the form of gender expression and clothing, motivation criteria in the form of encouragement and feelings of pleasure, context criteria in the form of positive things, not offending other parties and environmental conditions, risk criteria Benefit is a comparison of the amount of profit or loss that users will get after making disclosures.

In this study, the method used by users to manage their Instagram privacy is by deciding not to disclose their privacy at all on Instagram or creating a second Instagram account that is devoted to disclosing privacy. The second account used is only followed by people closest to and trusted by users which makes it more flexible to disclose their privacy.

Instagram users who actively use their accounts by uploading photos or videos as well as replying to comments or direct messages from followers, both women and men aged 18-25 with different jobs including students, students, and employees.

Generally, a person discloses to others gradually, starting from superficial things about himself to things that are personal and intimate. However, in this study, the self-disclosure process carried out by informants through Instagram social media tends to be done randomly and not gradually. On the main Instagram account, users include their real identities in their profiles. Informants 4 and 5 presented their full profiles and even added their employment or education status as well as their domicile to display a positive impression and increase their self-worth.

While on the other hand, Informants 1 and 3 explained that in displaying their profiles sometimes they made their accounts look anonymous or used names and profile photos that were not themselves. Informants do this to protect their identity at certain times, because according to them there are times when they do not want their real identities to be known. In the end, it can be seen that the control exercised by the informants in providing information which according to the informants is quite private about themselves in its own way.

Informants 2 and 3 chose not to share private information as much as possible or by using features provided by Instagram such as the hide story and close friend features which they can use to hide uploads from some of their followers. Informants 1, 4, and 5 actually chose to create a second Instagram account which they used as a special place to share more private information about themselves. In the research conducted by Pamungkas regarding CPM on the second account on Instagram, it also stated that informants filtered people who were allowed to follow and access their second account by implementing the protect/private feature and not everyone who sent follow requests would be accepted. Only people who are considered close and trusted by the informant can access this second account (Ultimate, 2019).

This account is also anonymous, which does not use the user's real name, photo and profile. When in an anonymous situation, a person will feel that he can express their true feelings and thoughts freely (Misoch: 2014). The view of rules contained in CPM theory distinguishes why individuals choose to stop or disclose personal information. Decision making to set personal rules has certain criteria such as cultural criteria, gender criteria, motivation criteria, contextual criteria, and risk or benefit ratio criteria (Griffin, 2012). The informants have applied the criteria of privacy rules and various ways in the process of disclosing themselves through Instagram. This can be seen from how all informants went through various stages of criteria such as culture, gender, motivation, context, and risk-benefit which were taken into consideration in making decisions to reveal themselves on their Instagram accounts.

The reason is that Instagram users carry out privacy management on their Instagram accounts because they want to feel safe about the misuse of their privacy information. In addition, there were experiences experienced by some informants in the form of negative comments. This study also found that the informants used various methods or their respective strategies when disclosing matters related to their privacy. As done by Informants 2 and 3 who use the features provided by Instagram such as closefriends and hide stories or form a second account. This is done because of the feeling of wanting to keep uploading their privacy and still having control over that information. In addition, the influence of the informant's experience when facing negative reactions to him.

The phenomenon of creating a second account by Instagram users is proof that they are revealing themselves and causing privacy that should not be for public consumption to be mixed into the public sphere. According to the informants, this was done because in their first Instagram account they only showed things from their best side that could make other people interested. Meanwhile, the second account is where they issue all their complaints and become their real selves. The researcher saw that the informants who used two Instagram accounts divided the roles and differentiated the information they shared. In the first account they form the best self-image and the second account is used to be who they really are.

Discussion

From the research analyzed, it can be explained that most users do not cover their identities such as names, photos, and profiles filled in according to their original data. However, this identity will be hidden at certain times. This can be done because they use CMC. Self-disclosure made on the main Instagram account focuses more on positive things to make people interested and like their uploads on Instagram. Users have different restrictions regarding the privacy they express on Instagram. In addition, they have different ways of disclosing their privacy. It can also be explained that the cultural components possessed by the informants and their environment affect the process of self-disclosure through Instagram. In the research discussed, it is explained that the audience analyzed takes into account the risks and benefits they will experience when making disclosures through Instagram.

Privacy basically must be owned by all humans with different levels of disclosure. Some have a fairly open disclosure of private information, some are quite closed. So it is necessary to apply the theory of communication management privacy to be able to better control communicators in sharing messages, especially in the current digital era where virtual identities are increasingly easy to see and record. In addition, by controlling privacy on social media, especially Instagram, it is expected to reduce anxiety in sharing information that can cause privacy violations. Therefore, it is necessary to understand *communication management privacy* so that every communicator can have knowledge in the selection of privacy information boundaries on their respective social media.

Based on the analysis conducted, it shows that every Instagram social media user has different goals when using Instagram stories which are part of the internet itself. From different purposes, the informants also have different privacy management rules as well.

They also do this privacy management arrangement based on five CPM criteria such as risks and benefits, motivation, context, gender, and culture. On the other hand, the informants also have their own strategy in setting their privacy by utilizing the features provided in Instastory, namely the delete feature that can be used before the content disappears after 24 hours, and the close friend feature.

This study also has limitations, including not all the results of the analysis data include what the majority of Instagram users' goals are for using the close friend feature. In future research, it is hoped that researchers can reach out to studies that have more diverse goals or focus on similar goals in more depth. In further research, the author hopes to explore more the application of *communication management privacy* theory to social media users, not only on Instagram. The author also hopes to increase the number of good informants, especially from the user side. This is expected to be able to find out in more *detail* in the application of *communication management privacy* theory by communicators in the use of social media in this era of increasingly rapid technological development.

References

Alhabash, S., & Ma, M. (2017). A Tale of Four Platforms: Motivations and Uses of Facebook, witter, Instagram, and Snapchat Among College Students? Social Media and Society, 3(1).

Beldad, A., Jong, M. De, Steehouder, M., Beldad, A., & Jong, M. De. (2011). The Information Society: An International Journal A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet A Comprehensive Theoretical Framework for Personal Information – Related Behaviors on the Internet. January 2015, 37–41.

Burgoon, JK, Parrott, R., Le Poire, BA, Kelley, DL, Walther, JB, & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. Journal of Social and Personal Relationships, 6(2), 131–158.

Child, JT, Duck, AR, Andrews, LA, Butauski, M., & Petronio, S. (2015). Young Adults' Management of Privacy on Facebook with Multiple Generations of Family Members. *Journal of Family Communication,* 15(4), 349–367. https://doi.org/10.1080/15267431.2015.1076425.

Child, JT, & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. Computer-Mediated Communication in Personal Relationships, February, 21–40.

De Wolf, R. (2019). Contextualizing how teens manage personal and interpersonal privacy on social media. New Media & Society, 146144481987657. https://doi.org/10.1177/1461444819876570

De Wolf, R., & Pierson, J. (2014). Who's my audience again? Understanding audience management strategies for designing privacy management technologies. *Telematics and Informatics,* 31(4), 607–616.

Denzin, Norman K. & Yvonna S. Lincoln. (2009). *Handbook of Qualitative Research.* trans. Dariyatno et al. Yogyakarta: Student Library.

Devito, J. A. (2012). *The Interpersonal Communication*. New York: Addison Wesley Logman Inc.

Gross, R., Acquisti, A., & Heinz, HJ (2005). Information revelation and privacy in online social networks. WPES'05: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 71–80.

Griffin, E. (2012). *In A First Look at Communication Theory* Eight Edition. America: McGrew Hills.

Hollenbaugh, EE (2019). Privacy Management Among Social Media Natives: An Exploratory Study of Facebook and Snapchat. Social Media and Society, 5(3).

Jones, E.E (1990). *Interpersonal Perception*. New York: WH Freeman.

Kuswarno, E. (2009). *Communication Research Methods: Phenomenology, Conceptions, Guidelines and Example of His Research*, Widya Padjajaran UII Central Library.

Littlejohn, S. W & Karen A. Foss. (2009). *Communication Theory*, Jakarta: Salemba Humanics.

Sugiyono. (2010). *Educational Research Methods Quantitative, Qualitative, and R&D Approaches*. Bandung: Alphabeta

Tubbs, S.L & Sylvia, M. (2005). *Human Communication*: Contexts of Communication, Editor Deddy (A Narrative Study of Author Status on Facebook, Communication Studies, Faculty of Social and Political Sciences, University of Indonesia: Jakarta.

Finn, R & Wright, David & Friedewald. (2013). *Seven types of privacy. European Data Protection: Coming of Age*, 3-32.

Jones, Edward & Pittman, Thane. 1982. *Toward a General Theory of Strategic Self Promotion. Psychological Perspectives on the Self.* 1(9). 231-262.

Liu, Z., & Wang, X. (2018). How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison. Information and Management, 55(8), 1005– 1023. https://doi.org/10.1016/j.im.2018.05.006

Lin, R & Sonya, U. (2017). *Self-disclosure on SNS:* Do Disclosure Intimacy and Narrativity Influence Interpersonal Closeness and Social Attraction? *Computers in Human Behavior,* 70, 426-436.

Mahardika, RD & Farida, F. 2019. Self-Disclosure on Instagram Instastory. *Study Journal Communication,* 3(1), 101 -117.

Masur, P. K & Michael, S. (2016). *Disclosure Management on Social Network Sites: Individual Privacy Perceptions and Use*

Oktarina, Y., & Abdullah, Y. (2017). *Communication in Theory and Practice Perspective*. Yogyakarta: Depublish.

Pamungkas, IR, & Lailiyah, N. (2019). Self Presentation of Two Instagram Account Owners on Account Main and Alter Accounts. *Online Interaction*, 371-376.

Petronio, S. (2013). Brief Status Report on Communication Privacy Management Theory. *Journal of Family Communication,* 6-14.

Petronio, S. (2016). Communication Privacy Management Theory. In CR Berger, ME Roloff, SR Wilson, JP Dillard, & D. Solomon, *The International Encyclopedia of Interpersonal Communication*,1-9).

Pitkänen, O., & Tuunainen, VK (2012). *Disclosing Personal Data Socially — An Empirical Study on Facebook Users' Privacy Awareness. Journal of Information Privacy and Security,* 8(1), 3–29.

Prasetya, MR (2020). Self-presentation and privacy awareness of micro-influencers on Instagram*. Journal of Communication Studies*, 239-258.

Rahadi, DR (2017). User Behavior and Hoax Information on Social Media*. Journal Management & Entrepreneurship*, 58-70.

Rahma, FO, & Prasetyaningrum, S. (2015). Personality to Inner Attachment Style Friendly Relations. *Psympathic, Scientific Journal of Psychology*, 153-168.

Rahma, S. (2019). The Influence of Motives for Using Instagram Second Accounts on Satisfaction live. *Communication Studies,* 259-267.

Ross, S. (2019). Being Real on Fake Instagram: Like, Images, and Media Ideologies of Value. *Journal of Linguistic Anthropology*, 1-16.

Serafinelli, ES, Cox, AC, Serafinelli, E., & Cox, A. (2019). *'Privacy does not interest me'. A comparative analysis of photo sharing on Instagram and Blipfoto 'Privacy does not interest*. A comparative analysis of photo sharing on Instagram and Blipfoto. Visual Studies, 34(1), 67–78. https://doi.org/10.1080/1472586X.2019.1621194

Thompson, J., Petronio, S., & Braithwaite, DO (2012). An Examination of Privacy Rules for Academic Advisors and College Student-Athletes: A Communication Privacy Management Perspective. *Communication Studies*, 54-76.

Umrati, & Wijaya, H. (2020). *Qualitative Data Analysis: Concept Theory in Research* Education. Makassar: Jaffray Theological College.

We Are Social. (2019). Global Digital Report 2019. New York: We Are Social.