Indonesia's Digital Native Perception of the Concept of 'Privacy'

RA Retno Hastijanti, University of 17 Agustus 1945 Surabaya, Indonesia
Alfa Layla Ahadina, Airlangga University of Surabaya, Indonesia

The Asian Conference on Arts & Humanities 2021
Official Conference Proceedings

Abstract
This study focuses on describing Indonesia's Digital Native Perception of the Concept of 'Privacy' concept in social media. The significance of this research is the case violations' high number of internet users' privacy, which have a serious impact on the aspects of security. It is chosen the digital native age group as the subject of the study because this group accesses the internet the most, especially social media. Then it is important to know the process of digital groups' natively interpretation of their privacy on the internet. This study uses descriptive research with a case study method. While The data collection technique is carried out by in-depth interviews. Next, it can be revealed some factors that important for digital natives and what they consider as their privacy on social media. Through this research has found that digital native has also experienced some inconvenience activities regarded the online media users and their reaction. Finally, it can conclude that it is needed a good public policy related to privacy in Indonesia and suggests the legal products disseminate related to privacy regulations optimally.

Keywords: Digital Native, Social Media, Privacy, Public Policy, Internet, Case Study

Preliminary

This research focused on Indonesian digital native's perception about privacy concept in social media. Research's interest in conducting this research is due to the increasing number of cases concerning the abuse of user privacy on the internet, especially in social media. Researcher realize that this phenomenon is a consequence of the presence of technology that helps human life, but that does not mean it should be underestimated. From a scientific point of view, this research is important to do, so that it can help the authorities in actualizing privacy regulations better.

This study provides a description of how are the perceptions of Indonesian digital native about the concept of "privacy" in social media. The subjects of this study are digital natives in Indonesia, which is in accordance with the definition of Prensky (2001), namely the age group who have lived with the internet since they started learning to write (p. 2). In Indonesia, those included in this group are millennial generation an generation Z, namely social media users who were born since 1980. The next criterion of the research subjects is that they must have used social media since childhood. Researchers want to see how this generation's perspective on the concept of privacy on the internet, especially social media.

This topic was chosen because according to research from the Indonesian Internet Service Providers Association (APJII) in 2018, currently 171.17 million people in Indonesia have been reached by the internet. In this number, internet users in Indonesia are dominated by millennial age groups and generation Z. The 20-24 year age group (generation Z) occupies the top position of internet users in Indonesia, with a penetration of 88.5%. Then followed by the 25-29 age group (millennial generation) with a penetration of 82.7%, the 30-34 age group with 76.5% penetration, and the 35-39-year age group with a penetration of 68.5%. Meanwhile, of the total internet users, 150 of them are social media users (Hootsuite, 2019).

According to Supratman (2018), digital native uses social media to obtain information, do the hobbies, communicate virtually, support lecture assignments, do online shopping, and adopt fashion styles and lifestyles. And it is interesting that digital natives can use social media at one time, in a multitasking manner (p. 52). Looking at this data, it is important to see how the digital native perceives the concept of privacy on social media. Remembering that a lot of their personal data is at a stake on the internet, especially social media. Currently there is no universal definition that describes privacy, so the researcher include several definitions of privacy according to several experts. Bogaert (2009) states that privacy is about people and their desire to be in control of how much access they want to give to others (hal. 195). Hal tersebut menunjukkan bahwa hak kontrol untuk mengatur privasi secara penuh dimiliki oleh individu.

This opinion is complemented by Hartono in Prabowo (1998), namely that privacy is a particular right o freedom (p. 17). Meanwhile, Rapoport in Prabowo (1998) defines privacy as the ability to manage interactions, the ability to obtain choices and the ability to achieve the desired interaction (p. 27). The urge to always protect one's privacy has emerged over time, since time immemorial. DeCew and Katsh in Woo (2006) explain that along with the development of civilization, society has various levels of enforcing formal rules, the concept of taboo, or other means in order to protect their privacy (p. 952). The beginning of the concept of privacy as legal right in modern life arose when Warren and Brandeis (1890) wrote a famous article entitled 'The Right to Privacy", which define privacy as 'the right to be left alone' or 'Right to be let lone' (Quoted in Woo, p. 954). Furthermore, the development of the modern

concept of privacu moves in line with technological developments that encourage public awareness that privacy is an important social value (Woo, 2006, p. 952). Discussion about privacy also include the issue that the government and media are present as external parties invading private space. The emergence of mass media also interferes with human privacy, for example, there is news about the private life of certain people, and so on.

Then, researchers consider it important to analyze public policies that discuss privacy, because at this time, privacy has begun to be commodified. According to Sevignani (2013), in his research entitled "the commodification of privacy", he states that almost all internet sites are commercial in nature, because in order to survive, these internet sites must remain profit oriented (p. 734). So, it will be increasingly dangerous for users who risk their personal data and privacy on the internet. In addition, cases of violation of privacy are also a concern of researchers considering that there are often various violations of privacy.

Coupled with technological developments, there are also many violations of privacy in the realm of cyberspace or the internet. This violation can be done by external parties, outside of someone's privacy. The researcher defines these external parties into 2 as stated by Woo (2006), namely the private sector and the government (p. 954). Woo (2006) explains that the discussion about privacy violations also includes the issue that the government and the media are present as external parties invading private space (p. 954). Researchers define "private parties" to be in between; the media, individuals, internet sites, online applications, and various service providers that operate using the help of the internet. Meanwhile in 1960, William L. Prosser, a well-known legal expert in his era, divided the four forms of privacy violations as follows (quoted from Sari, 2011, p. 20):

1. Intrusion

Intrusion is a violation of the right to privacy caused by interference with a person's physical ownership area which is legally protected. Intrusion can also be defined as the act of visiting or intervening in someone's personal area without being invited or without the person's permission.

2. Disclosure of Private Facts

Disclosure of Private Facts is a violation of the right to privacy caused by disclosure of information, resulting in a person having to bear the risk of being humiliated in the public at lrge (the potential to lower his standing in the eyes of the public) by his environment even though the disclosure of the facts is true.

3. Appropriation

Appropriation is a misuse of someone's name or likeness for certain purposes, namely for commercial purposes. Generally, this type of violation is found in cases of fraud, such as via telephone or Short Message Services. A breach of privacy in this form is a violation of which people were initially aware of the right to privacy. However, if the use of someone's name or likeness is not intended for commercial purposes then this can not be categorized as a violation.

4. False Light

False Light is a violation of the right to privacy caused by improper publication. By placing someone in the wrong place through the wrong description, misrepresenting someone with

another, visualizing someone with certain events or taking photos of someone that do not fit the context. Publication that confuses the crowd's view of a person is, of course, a violation of one's privacy.

Research Method

The research method used in this research is the case study method, where researchers only analyze certain case studies. In this case it is related to describing how digital native understands the concept of privacy on social media and how they perceive their privacy on social media. In accordance with the definition of Robert K. Yin (2003) that the case study research method is an emphirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used.

The step taken by the researcher to collect data was to conductan in-depth interview with the help of an interview guide, namely a list of open questions. The purpose of open questions is that there is no attachment between the researcher and the wuestions that have been compiled, but the researcher is free to develop the topic of conversation as long as it is related to the topic (Mashud, 2005, p. 5). After obtaining data from interviews with eight informants, the researcher made a trascript by writing down the entire contents of the conversation during in-depth interviews. The eight informants were selected on the authority of the researcher in exploring the informants. The researcher tries to find various informants' backgrounds so that various data appear. Then the researcher sorted out the appropriate interview results, and had a focus and attachment to the research topic so that they could answer the problem formulations in this study.

Technically, researchers collect elements of privacy according to various country regulations in the world, namely the Indonesia National Regulation for Electronic Information and Transaction Law, The European General Data Protection Regulation, The Canadian Digital Privacy Act, and The Privacy Act 1998. Later, these elements will become the points of interview with informants. Through this, the researcher wants to see what elements are considered as privacy by digital natives. Researchers found that among all these regulations, the things that generally considered as an element of privacy are: information about family, sensitive information, sexual preferences, health information, sexual preferences, health information, personal financial conditions, and complete personal data or personal identity.

Discussions and Findings

The results of this study were summarized by the researcher into four parts, including: digital native meaning of the concept of 'privacy' in social media, independent privacy protection strtegies on social media by digital natives, digital native opinions regarding the direction of government policies related to privacy issues in Indonesia.

1. Digital Native Preception About the Concept of "Privacy" in Social Media

In this study, the researcher summarizes the answers to digital native perceptions in Indonesia into several parts, namely; digital native interpretations of the concept of privacy on social media, independent privacy protection strategies on social media by digital natives, digital native opinions on violations of private data on social media by external parties, and digital native opinions regarding the direction of government policies regarding privacy issues in

Indonesia. From the interview results, it can be found that digital natives interpret Personal Health Information, personal data, misfortune, personal financial conditions, and sexual orientations as things they consider their privacy on social media. Informants do not want these things to be known by the general public againts the will of the informants. The conclusion was obtained after the researcher summarized the privacy elements in various privacy regulations in the world, and then explored the informations' perceptions regarding these elements through the in-depth interview method. Of the 5 (five) elements approved as privacy by the digital native above, only 2 (two) of them have been explicitly regulated in the Law by the Indonesian government, namely personal financial conditions and Personal Health Information. In Indonesia, the government comprehensively regulates policies regarding personal health information. Protection of personal health information focuses on patient medical record data, which from the very beginning according to Law no. 29/2004 on Medical Practice, has qualified as data that should be kept confidential. In Indonesia, the financial condition of the population is regulated in the Banking Law, namely Law No. 10 of 1998 which regulates issues related to bank secrecy, which obliges banks to keep everything related to data and information about customers confidential, including financial conditions. Or personal information, including accounts payable. Banking Law Article 1 Paragraph 28 iterprets bank secrecy as anything related to information regarding depositing customers and their deposits. Meanwhile, most of the digital natives don't know this, because they only know the ITE Law as the only regulation that regulates privacy.

2. Independent Privacy Protection Strategy in Social Media by Digital Native

Then, this study found the existence of privacy protection tactics that are typically used by digital natives on social media. Privacy protection is a strategy carried out by digital natives in order to get around tha process of sharing their privacy on social media. Researcher discovered digitl native's tactics about sharing content on social media privately, in order so that their privacy is not widespreaded. These methods include creating a second account, creating an anonymous account, adjusting audience reach settings for uploads on social media to protect privacy, and locking his account on social media. Second Account is a term for a side account that is owned by a social media user along with the main account, in the same social media application. The second account still displays some of the user's real identity, but is not as complete as the main account. Second account is usually locked to To follow a second account, approval from the account owner is required. According to Dewi and Janitra (2018), the reason users create a second account is accompanied by the hope of getting certain ratings, because some people feel like presenting themselves in another version (p. 340). Anonymous accounts are accounts on social media that do not reveal the real identity of the owner. Derived from the word anonymous, which according to the Cambridge Dictionary is "something that is made or done by someone whose name is not known or not made public and having no unusual or interesting features" [quoted from www.dictionary.cambridge.org]. So, anonymous accounts are used by users to acces certain things without wanting these activities to be known by others. Meanwhile, according to Kurnia (2017), anonymous accounts, fake accounts, and other obscure accounts are people who write, have opinions, use social media and want to do activities in cyberspace without wanting to know their personal identity by others (p. 192). Social media content is something that is uploaded to someone's social media account. The Merriam Webster site defines content in general as the main substance such as writing, illustrations or music that is available and accessible via internet [quoted from www.merriam-webster.com]. Contents on social media can be in the form of pictures, videos, music, and writings. Later, fellow social media users can exchange comments and give likes to the content. Later the digital natives can upload various kinds of their daily lives, including their privacy

through the contents. In this study, researchers captured the fact that digital natives often share their privacy, but with the audiences they have selected. Researchers have again discovered a strategy used by digital natives in order to protect their privacy on social media, namely the use of a locked account feature. This strategy is supported by features in the social media application. If a user locks his account, then the account will not be freely accessible by other users. With locked accounts, digital native can curate anyone who can participate in it. Prospective followers who want to follow an account must request a request first. Only when the request is approved by the account owner, potential followers can become followers of the account. Researchers found a native digital activity carried out in order to protect their privacy regarding old content on social media. Digital native tries to edit legacy content on socil media to suit the current living conditions.

3. Digital Native Opinion Agaainst Violations of Private Data of Social Media Users by External Parties

Researchers will also analyze the privacy disturbances experienced by digital natives n the internet in general, and in social media n particular, and how digital natives respond to this. William L. Prosser in Overbeck (2017) explains four concepts of privacy violations, namely intrusion, disclosure of private facts, and false light (p. 184). According to Sari (2011), these violations are included in the types of violations against the Privacy of Person's Persona (p.21). In addition, there is also a violation of the Privacy of Data About a Person, namely a violation of the privacy of personal data about a person that is collected and used by other people. In this study, researchers found that the informants had experienced three types of violations, namely data leakage on online platforms, misuse of telephone numbers, and cases of False Light violations. In addition to the case of the sale of personal data from users, which is widely known to be carried out by social media Facebook, at the time of writing this research, there was widespread news about the leakage of 91 million data from the e-commerce company Tokopedia. Tokopedia is the largest e-commerce platform from Indonesia, which is engaged in online shop platforms. Meanwhile, the bsence of a digital native initiative to sue or protest to Tokopedia regarding data security also proves that in general, digital native awareness is still low to take this action. They generlly convey that taking the advocay route to protect personal data is a difficult and "complicated" thing to do. One of the cases of privacy violations that often occurs in Indonesia is the terror SMS (Short Message Service) experienced by the owner of a telephone number. SMS terror is in the form of fraud or offers of money loans with certain interext. Generally, victims are terorrized after registering their number with a bank, certain organization, or even shortly after making prepaid registration. In fact, with the obligation to conduct prepaid registration before using a telephone number, the Ministry of Communication and Information (Kominfo) hopes to reduce fraud cases. Reported by Makki (2018), the perpetrators of the fraud were suspected of getting the phone number from individuals who worked for organizations that had lots of contact with clients' personal data [quoted from www.cnnindonesia.com]. Responding to this, in this study it can be concluded that digital native is aware or understands that misuse of telephone numbers is a violatoin of privacy. However, all of the informants did not care about this because the informants did not feel that they had received direct threats in the real world even the informants tended to rarely use the SMS application on their cellphones. And also there are no precautions from digital natives against the dangers of miuse of phone numbers. Next, there is also a type of violation in the form of False Light. According to Kenneth (2013), False Light is a violation of privacy caused by improper publication (quoted in Sari, 2011, p. 20). The RT informant who was a college artist had experienced this, namely that he was placed in an incorrect description.

Publications that confuse people's views of someone are a form of privacy violation (Sari 2011, p. 20).

4. Digital Native Opinion About Direction of Government Policy Regarding Privacy Issues in Indonesia

Then, the researchers asked their opinion on the privacy regulations in Indonesia. They generally answered that the government, especially the Ministry of Communication and Information, tended to be lacking in efforts to promote or socialize the prevailing regulations. The researcher concluded that the informants only know the ITE Law as the only regulation regarding privacy in Indonesia, and do not know further about the details of the articles in it. Informants also have suspicions about the ITE Law which is often problematic. They know this from several news on the internet about victims of the ITE Law. In the perspective of political communication, according to Sidharta in Sudjana (2016), the state as a law enforcer should carry out legal education and civilization which is generally aimed at all people (p. 127). This includes increasing the use of more modern communication media in the implementation of legal counseling that can support the acceleration of the dissemination, knowledge, understanding and appreciation of the law (Sudjana, 2016, p. 127). Concrete steps, such as immediately passing the personal Data Bill (RUU), also need to be taken by the government, given that technology is increasingly sophisticated and citizens are also growing. Given that not only Europe, currently other countries such as Australia, South Korea, Thailand, and Brazil also have regulations similar to the GDPR [quoted from www.theconversations.com]. In addition, researchers found that there is a habit of digital natives not to read privacy policies when they want to log into certain accounts on a social media platform. All of the informants said that they immediately pressed the button "I have read and understand the existing privacy policy", whithout actually reading it. In fact, it is through this option that the personal data of social media users is at stake. There needs to be socialization from the government regarding this matter, regarding the procedures for protecting personal data on social media.

Conclusion

Through this research it is known that informants interpret Personal Health Information, personal data, misfortune, personal data, personal financial condition, and sexual orientation as things they consider their privacy on social media. Informants do not want these things to be known by the general public againts the will of the informants. The conclusion was obtained adter the researcher summarized the privacy elements in various privacy regulations in the world, and then explored the informants' perceptions regarding these elements through the in-depth interview method. Of the 5 (five) elements approved as privacy by the digital native above, only 2 (two) of them have been explicitly regulated in the Law by the Indonesian government, namely personal financial conditions and Personal Health Information.

Both are regulated separately through two legal products, namely the Banking Law No. 10 of 1998 and Law No. 26 of 2009 concerning Health. In both laws, there are points that require banks or health care agencies to protect banking data and health care patients, but they do not explicitly regulate its distribution on the internet. So the researchers conclude that an integrated legal umbrella is needed which can explicitly define and regulate data / information that is considered privacy by internet users, and is able to protect if at any time the user's privacy is misused.

In this study, researchers found that educational background, occupation, place of residence, and age affect how informants engage in social media activities. The informant's life background forms a mindse that influences how they build their self-image on social media. Digital natives who have worked tend to try to be more careful in expressing themselves on social media, so that their work clients will look well. Meanwhile, informants who are still in school or college age and are not currently working tend to use social media as a means of expressing themselves properly in front of their social evirontment, whithout any encouragement to look good in front of cliets / colleagues.

Then the researcher found a similarity among all informants, namely, in the use of social media, all informants were equally trying to manage their privacy as best as possible. Informants carry out several unique activities to protect their privacy on social media independently. This is supported by a number of features provided in social media, such as; an account locking feature, a feature that allows to sort out content audiences, as well as a feature that allows editing old content on social media. The informants took full advantage of these features which were shown in several activities. Researchers define this activity as an independent privacy protection strategy on social media.

These strategies include creating a Second Account, creating an anonymous account, using the Locked Account feature and setting audience reach settings on uploads on social media as an effort to protect privacy, as well as editing legacy content on social media. Examples are informant Nisa who still shows her misfortune in the close friend feature, RT informant who uses an anonymous account to watch pornographic content on Twitter – so that her friends don't know her on the main account – and informant Ahmad who hides activities related to gay sexual orientation which is stigmatized by the community in the close friend feature.

This is in accordance with the Rapoport in Prabowo (1998) which defines the concept of privacy as the ability to manage interactions, the ability to obtain choices and the ability to achieve the desired interaction (p. 27). Referring to this definition, the researcher concludes that informants carry out privacy management in order to create the interactions they want on social media. This management is reflected in the privacy protection strategy independently carried out by informants on social media. Then the researchers managed to collect digital native opinions on the private data breaches of social media users. It is known that there are 3 (three) cases of violations that have been experienced directly by the informants. These cases include data leakage on Tokopedia e-commerce, cases of misuse of telephone numbers, and cases of False Light.

In the case oof data leakage from Tokopedia e-commerce users, the researcher found that the opinion of the informants tended to vary. Informants who are younger (17-18 years) tend to ignore cases of data leakage, and do not take special steps to avoid misuse of their data. Unlike an informant who has an urban background and has more knowledge about the importance of protecting personal data, namely the RT informant, who immediately carried out preventive activities by changing his password on social media, for security. There is also the opinion of informant Zzyafra who does not care at all if the data is leaked on the internet, as long as she can still get the benefit from the internet service provider, which in this case is the transaction through the Tokopedia account. This is consistent with research conducted by Woo (2006) that most of the internet users tend to voluntarily risk their privacy as long as they get some material compensation (p. 952).

In response to the leakage of telephone number data, which led to the SMS terror case and fraudulent telephone calls, all informants agreed that this did not worry them. The informant argues that as long as the informant is not deceived and loses money in the real world, there is no need to report the case to the authorities. Meanwhile, in the case of false light that befell the RT informant, the researcher found that the RT informant had resolved the case well. He contacted the online media that published false news about him, and asked that the news be deleted. The RT informant did not use Article 26 paragraph (3) and (4) Law Number 19 Year 2016, because apart from not knowing about the article, he also did not want the case to be more complicated. The informant's opinion led the researcher to the conclusion that digital native informants tended to underestimate the security of their personal data spread on the internet. Even though they consider personal data as privacy, they tend to be lazy to secure it or do advocacy regarding data protection in the realm of law.

This research also summarizes the opinions of informants regarding the direction of privacy-related policies in Indonesia. The resercher found that the majority of informants understood the ITE Law as a legal product that has so far been used by the government to regulate privacy. Informants tend not to know other public policies, apart from the ITE Law. Researchers also found a tendency that informants were suspicious or dissatisfied with the performance of the ITE Law. This is strengthened by the opinion of RT informants who think that the ITE Law is a tool used by the government to attack citizens who convey criticism. Meanwhile, the FD informant wants the government to conduct socialization related to laws that regulate privacy, so that their insights regarding privacy regulation can increase.

Researchers suggest that the government optimize the use of more modern communication media in the implementation of legal education in order to support the acceleration of the spread, knowledge, understanding and appreciation of the law (Sudjana, 2016, p. 127). The researcher also advised the government to immediately pass the Personal Data Bill, given that technology is increasingly sophisticated and the number of citizens using internet continues to grow, as well as the number of recent cases that threaten the privacy of the wider community that occur on the internet, especially social media. If the discourse on the Personal Data Bill is successfully passed by including a clear definition regarding the limits of the user's personal data, while establishing a reliable protection mechanism, then there will be a bright spot in the intricacies of protecting the privacy of the Indonesian people, especially in the sphere of the internet.

References

Andi., 2019. *Hootsuite (We are Social): Indonesian Digital Report 2019.* [Online], available at: https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2019/ [Accessed 28 March 2019].

Canares, M. (2018). *Online Privacy: Will They Care? (Teenagers Use of Social Media and Their Understanding of Privacy Issues in Developing Countries).* Boston: World Wide Web Foundation.

Diamond, M. (2002). Sex and gender are different: Sexual identity and gender identity are different. *Clinical child psychology and psychiatry*, *7*(3), 320-334.

Forsyth, D. R. (2010). Group dynamic. Belmont: Cencage Learning.

Ida, Rachmah., 2018. *Studi Media dan Kajian Budaya*. Jakarta: Prenadamedia Group.

Justice Law Canada. (2010, Mei 6). *Criminal Code Privacy Act*. Retrieved Mei 5, 2020, from Justice Law Website of Canada: https://laws-lois.justice.gc.ca/eng/acts/C-46/

Korobkova, K. A., & Black, R. W. (2014). Contrasting visions: Identity, literacy, and boundary work in a fan community. *E-learning and Digital Media*, *11*(6), 619-632.

Lindlof, T. R., & Taylor, B. C. (2017). *Qualitative communication research methods*. Sage publications

Prensky, M. (2001). Digital natives, digital immigrants. *On the horizon*, *9*(5)

Prensky, M. (2009). H. sapiens digital: From digital immigrants and digital natives to digital wisdom. *Innovate: journal of online education*, *5*(3)

Rockwell, D, Giles, D,C. 2009. Being a Celebrity : a Phenomenology of Fame. Journal of Phenomenologycal Pscycology 40. No : 170 – 210

Rodgers, S., & Harris, M. A. (2003). Gender and e-commerce: An exploratory study. *Journal of advertising research*, *43*(3), 322-329

Supratman, L. P. (2018). Penggunaan Media Sosial oleh Digital Native

Tapscott, D. (2009). Grown up digital: How the net generation is changing your world. New York, US: McGraw-Hill

Woo, J. (2006). The right not to be identified: privacy and anonymity in the interactive media environment. *New media & society*, *8*(6), 949-967.

West, R., & Turner, L. H. (2018). *Introducing Communication Theory: Analysis And Appliaction*. McGraw-Hill Education.

Whittaker, E., & Kowalski, R. M. (2015). Cyberbullying via social media. *Journal of school violence*, *14*(1), 11-29