University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

Users' Awareness of Personal Information on Social Media: Case on Undergraduate Students of Universitas Indonesia

Rahmad Nur Iman
University of Indonesia, rahmad.j500@gmail.com

Taufik Asmiyanto
University of Indonesia, tasmiy@ui.ac.id

Muhammad Hanif Inamullah
University of Indonesia, hanif.inamullah@gmail.com

Users' Awareness of Personal Information on Social Media: Case on Undergraduate Students of Universitas Indonesia

Rahmad Nur Iman[1], Taufik Asmiyanto[2], M. Hanif Inamullah[3]

[1]Undergraduate student of Library Science, Faculty of Humanities, Universitas Indonesia. Indonesia
[2,3]Department of Library and Information Science, Faculty of Humanities, Universitas Indonesia. Indonesia

Abstract

Posting a personal data information on social media can be easily done by anyone. These activities are easily found on the user's social media profile page, which is not uncommon to contain personal information. This is coupled with the possibility of security gaps in social media services, can be utilized for various purposes, and by anyone, including other users and service providers themselves. On the other hand, regulations and policies regarding personal data information, have not been clearly regulated in Indonesia. By using a qualitative approach, this research aims to determine the stage of the user consciousness related to personal data information, and a variety of personal data information that is listed on the user's social media. The results show that the stage of consciousness arises when the user thinks critically in the decision of the inclusion of a personal data information. The results of the study also showed that users know a variety of personal data information, which is appropriate for each user's background. This research also suggests that the social media users should provide themselves with the sufficient knowledge of social media usage.

Keywords: *Personal data information, Privacy concerns, Social media, User awareness*

Introduction

Social Networking Service (SNS) or commonly known as social media has become the most popular platform for users to share information online. Its users have grown rapidly during the last decade with Facebook, Twitter, Instagram and many other types of this platform. It has been used by most of the world citizens with various background and age for various purposes, including finding and keeping in touch with old friends, networking with people with mutual interest, and dating (Quan-Haase, & Young, 2010). Social media is defined as web-based services that allow individuals, communities, and organizations to collaborate, connect, interact, and build community by enabling them to create, co-create, modifies, share, and engage with user-generated content that is easily accessible (Sloan, L., & Quan-Haase, A, 2017). As many kinds of information created and spread on the internet, social media has become one of the most contributing platforms to it. With so many user-generated contents available, data in social media have become an appealing platform to be used by organizations for various purposes, such as providing personalized online services and features as well as for malicious purposes such as data theft and various other crimes.

Despite of the popularity of social media, privacy concerns have been arising for this platform over the past years. Social media enables people to share information not only to one particular person, but also to public. Consequently, various individuals' data is spreading in the public

sphere on the internet, both in the nature of public domain information and personal information. The large amount of user data circulating on social media may carries the risk of exposing the individuals both consciously and unconsciously (Beigi & Liu, 2018). Many social media users are unaware of what kind of information they actually share on social media. They often do not realize that they maybe expose their privacy to public. Sometimes they voluntarily share their personal information on social media in various forms, including text, images and videos. For example, users may post and share their family vacation photos on Instagram, including its tagging to the places they visited and the people that join their vacation without realizing that the information could be used and exploited by some people or organizations for various purposes, including barging into their empty houses. There have been many cases of the leaking of personal information on the internet, including the case of Facebook users' personal data leaks which is rumored to have been sold to companies for user interests-based advertisements[1].

The disclosure of personal-related information could lead to many negative impacts for social media users, especially related to the risk of the misuse of their personal information. Therefore, this paper aims to discuss how social media users are aware of the disclosure of their personal information related to privacy issues that they might face.

Research on awareness of privacy issues on social media have been discussed in the previous years. A research conducted by van Eecke and Truyens (2010) states that many social media users are not aware that the use of social media has impacts on the exposure to their personal information and many social media users are not aware that it has an impact on privacy issues for their colleagues and families. Furthermore, van Eecke and Truyens also discussed the complexity of implementing the EU Data Protection Directive in a social media environment at that time. A comprehensive study was also conducted by Kumar et al (2016) to more than 200 respondents to identify the privacy concern that social media users can undertake before they to prevent any privacy violation. The result shows that concerns over privacy issues is still lacking among social media users. Thus, this have an impact on the efforts made by users to enhance the security of their social media accounts.

Thus, the objective of this research is to identify the stages of awareness and variety of personal information embedded on social media by individuals at the higher education level. This paper is also expected to enhance the understanding of the importance of managing personal information of social media users in Indonesia, so that readers as community representatives become more selective in sharing personal information in their social media accounts.

Methods
This research was conducted using a qualitative approach with a constructivist paradigm to describe the awareness of social media users of their personal information. To gather the data,

---

[1] Griffin, G. (2018, April 24). *Facebook is in Crisis Over Data Abuse Scandal and Harvesting of Information was Rife, Says Academic at Heart of It*. The Independent. Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-data-abuse-scandal-latest-cambridge-analytica-kogan-a8320066.html

eight undergraduate students from several different majors were selected and participated in the research using convenience sampling method and interviewed with open-ended questions. The interview questions including information about their profile and questions related to research topic such as personal information, social media, and privacy. This paper will analyze the collected data with emphasis on three main topics, *the understanding of personal data*; *the consciousness of personal data sharing*; and *the privacy concern of social media users*.

Understanding of Personal Information

Personal information is any kind of information related to a person, including name, contact details, hobby, physical and health details and anything that can identify the individual. One of the participants of this research interpret personal information as all information about themselves. This interpretation about personal information is in line with Lupton et al idea which states that personal data dealing with very intimate information about individuals (Lupton Pink, Labond, & Sumartojo, 2018). Furthermore, EU General Data Protection Regulation defines personal data as any information which are related to an identified or identifiable natural person. Which means that the data subject can be identified by the identifier including name, ID number, address, online identifier or even appearance (EU GDPR, 2018).

Meanwhile, another participant argued that personal information is everything related to one's personal life. When associated with social media, various individual activities and personal life can be shared over social media platforms. These activities shared in social media will produce data. An individual's personal life can be depicted in detail when data has been accumulated, be it by governments, companies or other users (Altman, Wood, O'Brien, & Gasser, 2018). This illustrates that activities in social media can be categorized as personal information, because they can describe personal life. Furthermore, in social media, users often upload expressive and emotive things, producing rich and detailed information related to a person (Pangrazio & Selwyn, 2019). Even though they do not upload attached personal data like an ID card number, individuals can still be identified through their personal life.

Personal information can also be identified based on the characteristics of the data. This was conveyed by one of the participants who stated that personal information is related to confidential personal data. The assumption that personal information is private, important and confidential is true. In the context of personal data protection (PDP), personal data information fundamentally has the right to personal life and the right to protection. Therefore, the existence of personal data as personal, important and confidential data naturally arises because of the ownership of the data and the existence of protection against it. thus, it is difficult to explain ownership of data without explaining ownership related to personal data (Janecek, 2018).

Some of the participants also identify personal information by giving examples of personal data including phone number, address, email, parent name, age, place of birth and birthdate, ID card number or driving license number, password, social media username, and name of attended school or university. Some of them also stated that this information should not be shared publicly. Most of these examples can be used to identify individual identity. As

mentioned earlier in this paper, EU General Data Protection Regulation stated that personal data refers to any information relating to an identified individual or an identifiable individual (EU GDPR, 2018). Phone number, address, and email address were the mostly conveyed by participants when asked about the example of personal information. Based on these responses, it can be seen that various kinds of personal data information on social media, often originated and have a connection with individuals in the real life. Furthermore, numbers from personal cards such as ID Card, driving license, and student numbers are also classified as identification numbers which contain personal information. Patrick Breyer stated that information on these numbers will still be considered personal data, although it may not necessarily and directly refer to a specific individual (Dove, 2018). Therefore, this number, along with other numbers (such as health card numbers, vehicle and number) are protected by law (EU GDPR, 2018).

Social media user ID or username and password are also categorized as personal information because the username or user ID can be easily identified and matched with real name of the user in a database of a service. While password is a secret code based on letters or numbers which is still dominantly used until today (Li, Wang, & Sun, 2017). However, humans have limited memory, so most of people use a combination of passwords that are easy to remember. It is commonly known that users often use their personal information such as their birthday as their passwords, which creates a risk of password leaked (Li, Wang, & Sun, 2017).

In addition, information about the place where we work or study can be classified as personal information. Because if this data is combined with other data can produce sufficient ability to identify individuals (ICO., 2018). In Recital 21 by GDPR, all information from data that can identify certain individuals, either directly or indirectly, deserves to be protected (Dove, 2018).

Users as individuals often leave information categorized as personal data when using the internet, especially social media (Cavoukian, 2019). People nowadays also seem too enthusiastic in sharing their personal information widely on social media with other users (Tavani, 2013). Thus, nowadays personal information is not only important things such as phone numbers, ID number or home address but also includes social media post related to personal life such as location data, favourite things, or health data (Tavani, 2013).

The massive amount of personal data on the internet causing changes in the nature of the data itself. Various types of personal data can generally be classified as non-public personal information (NPI), because it is sensitive, highly confidential, and very personal (Tavani, 2013). Information on sensitive data in the NPI including physical or mental health conditions, ethnic or racial origin, genetic data, fingerprint data (biometrics), and personal beliefs like religion. In general, this type of information is data that can be related to the types of discrimination discussed in human rights instruments and constitutional protection related to the right of non-discrimination (Privacy International, 2018).

On the other hand, public personal information (PPI) is information about individuals that is neither confidential nor highly sensitive. PPI contains information about a person, such as where you work or study, or the type of vehicle you drive. PPI includes information, but does not rule out other possibilities, namely; positions in public institutions, online shopping lists,

classroom attendance lists, etc. that can still refer to individuals as private. However, the information content in PPI that describes or refers to a person does not receive the same treatment as the NPI (Tavani, 2013). This is because information about personal is categorized as public information. In addition, the information contained in the data on the commercial sector is treated to the point that there is no longer any protection against it (Nissenbaum, in Tavani 2013). This is also due to the fact that existing regulations still focus on NPI data (Tavani, 2013).

Consciousness of Personal Data Sharing

At this point, it was known that some participants experienced a critical thinking stage in the inclusion of personal information. By going through the critical thinking stage, the participant has control over his consciousness in the inclusion of personal data information. Some of the participants stated that they only use social media for pleasure. Sometimes they post an update on their social media account to show or see affection from other users. It is commonly known that one of the purposes of using social media is for seeking pleasure. This was also conveyed by Hui, that social media providers are known to be able to exploit users' pleasure in submitting personal data information (Krasnova et al., 2010). In fact, individuals often share their personal information by posting their photos and disseminating it on their social media pages (Krasnova et al., 2010). This sharing activity is carried out based on a value, one of the values is the enjoyment of communicating through social media (Muniz and O'Guinn in Krasnova, et al., 2010). Some parties see that social media is a place to share pleasure or enjoyment and leads to the opinion that social media is only used for this purpose (Rosen and Sherman in Krasnova, et al., 2010). In terms of pleasure, most of the users are considered to not think critically while posting their personal information when using social media.

Aside for a mere pleasure, other participants argues that they also use social media for sharing their knowledge and experience. There is a personal desire to share information with the intention of describing themselves by sharing their achievements, experiences and activities using social media (Krasnova, et al. 2010). This means that they consciously thinks to share good things which can represent themselves well on social media. Meanwhile, the others said that they start to limits information sharing activities on social media as they are aware that the information can be consumed publicly. This is related to the possibility of a privacy violation in social media, whether committed by people we know or not (Krasnova, et al. 2010). The relationship of a social media user with his real life friends definitely have a higher level of trust compared to strangers they know on social media. Ridings explained that in general, uncertainty in the negative impact of activities on social media is caused by not knowing other users visually (Krasnova, et al. 2010). In such conditions, users do not have the ability to monitor each other's users in their social media, and they must implicitly trust those users.

Another participant revealed that he was quite selective in giving his personal information. tailored to his needs and other party needs. Based on Gibbs, the intention to develop friendship on social media, sometimes strongly involves disclosing information (in Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). This is reinforced by the opinion of Lampe et

al. including personal data information, it will also send a signal that triggers other people to respond (Lampe et al., in Krasnova et al., 2010). According to Gibbs statement about interpersonal relationships, the intention to develop friendship on social media, sometimes strongly involves disclosing information (in Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). This is reinforced by the opinion of Lampe et al., where users who enter their personal data information will also send a signal that triggers other people to respond (Lampe et al., in Krasnova et al., 2010).

Other participants stated that they uses social media to build relationships with others, or get rid of boredom and express themselves. Furthermore, several participants also stated that they shared personal information on social media with the aim to build personal branding. They tried to portray their individual characteristics in social media to build their good personal image and trust. Social media is a place where people can do many things. Krasnova et al. (2010) summarized several intention of individuals reveal their information when interacting on social media, namely; relationship building, as a place for self-presentation, and a place for enjoyment. With the consciousness and ability to think critically, individuals also have the ability to direct the goals of what they do. In social media, it is possible for users to do something with their personal information, including sharing it. Activities such as sharing of personal information lead to self-disclosure. Self-disclosure is an activity of disclosing personal information to others for inter-individual understanding, intimacy, and trust in interpersonal relationships (Varnali & Toker, 2015).

Regarding consciousness, another thing that was also discussed by participants was the security risk in social media. Some participants stated that they do not include highly personal information such as phone numbers or addresses on social media like Instagram. Some also take even more aggressive security measures by locking their Facebook accounts and deleting posts that contain personal information on them. Inclusion of personal information on social media is indeed very risky (Okditazeini & Irwansyah, 2018). Knowledge of this risk will arise when users subjectively become aware of the unwanted dangers of including information from their personal data (Smith in Yeh, et al., 2018).

Social media can be very useful for users as it eliminates economic and geographic boundaries, and can also be useful for achieving goals in terms of work, entertainment, and education (Okditazeini & Irwansyah, 2018). In its use, it encourages users to include their personal data information (such as phone numbers and locations) (Milham, 2018). Users may not include confidential things such as home address, but they often include relevant information in certain contexts (Boyd in Okditazeini & Irwansyah, 2018). In terms of risk, individuals as users have vulnerabilities, if they provide too much personal data information on social media may lead to high risk for its users.

Privacy Concern of Social Media Users

Privacy concern in sharing personal information on social media may arise because of the consciousness and awareness of potential risk of users. One of the participants expresses his

concern someone may use their personal information, including photos and claim to be himself and committing crimes in social media. This concern arises due to the experience and the possible negative impact on their personal information. Most of the participants also stated that they were worried about the misuse of their personal data information on social media. This form of abuse can be various, for example, for fraudulent activities with various purposes.

However, several participants also admitted that many people do not care about their personal information on social media. Sometimes, they only want to follow trends on social media without thinking about the risks and dangers they may face by sharing personal information on social media. A participant argues that there is an urge in nowadays generation in following trends and the need of acknowledgment from other social media users. In this regard, a case of a 17-year-old teenager in the United States was arrested because he uploaded a photo of himself and the item he stole can be a proper example (Yu, 2014). This shows that education related to social media is needed. In addition, the responses from participants indicate that an account could be taken or stolen because the content of personal data information invites other users to do so. Although the inclusion of personal data information is not something that leads to wrong action, it does lead to risky behavior (Yu, 2014). Previous study indicates that 42% of university students experienced several types of privacy issue while using social media (Henson in Okditazeini & Irwansyah, 2018).

Another case of privacy threat experienced by one of the participants. She said that some strangers save her photos uploaded on social media. She worried that those pictures are used for inappropriate purposes. As stated in a previous part of this paper, anything or any information that lead to identification of individuals can be categorized as personal data, including personal photos. The participant said that saving photos of themselves could lead to the use of personal data. Livingstone argues that users are aware of potential threats to social privacy such as theft and misuse of photos and have some level of anxiety regarding their privacy (Dhir, et al. 2017). In Van Dijck's research, it is known that photos shared over the network can easily consumed by public (Dhir, et al. 2017). Other potential threats were also conveyed by other individuals as social media users, stating that some parties have the ability to exploit security gaps. This opinion is also supported by a statement submitted by the Federal CIO Council in 2009 which showed that social media services are vulnerable to cyber attacks, one of which is Spear Phishing (Dhir, et al. 2017). Spear Phishing is a phishing attack that has been modified and targeted at an individual or multiple individual (Bossetta, 2018), which can direct an individual as a user to visit a fake website page and request log-in related information (Ho, et al. 2017).

Apart from being concerned about potential violations by other social media users, participants were also concerned about potential privacy threat that might be committed by the social media provider itself. They are concerned that their personal data is being used or sold to other parties without the consent of the user. Brunton and Nissenbaum (in Pangrazio & Selwyn, 2019) describe it as information asymmetry, which means circumstances in which our data is collected in conditions we may not understand, for purposes we may not understand, and in ways we may not understand. Such data collection activities are called data mining.

Information about individuals is often obtained from implicit things when looking at patterns in these data (Tavani, 2013).

However, the activities carried out by social media service providers related to this privacy issue have been realized by some users. One participant stated that he knew that social media like Instagram could see its user algorithm, and this had been regulated by the End User License Agreement (EULA) when he signed up on the social media. The need for algorithms is intended to see a certain picture regarding individual interest in something. Data from this algorithm is collected based on user activities during social media activities. In a case of personal data, users often produce it unconsciously and have little understanding of where, how, or why the data was collected (Pangrazio & Selwyn, 2019). This applies to social media, where users often share photos, location, email address, when interacting with social media.

On the other hand, Tavani (2013) also argues that information regarding online shopping transactions can be combined with other shopping-related information for websites to create consumer profiles. This means that information combined with other relevant information will be able to produce new information. This new information has more than one value or benefit. The use of algorithmic data by social media providers can be used for various purposes and objectives based on a value. This value will encourage the holder of this information to do something that he considers profitable, such as selling it to third parties.

In the context of social media, users are concerned about the use of a combination of information through certain algorithms, which indirectly has an influence in producing content on their social media according to the user's algorithm. Users also worry that social media providers are able to control the activities that users carry out in social media. for example, through suggestions conveyed by advertising intermediaries that appear on the user's social media home page. Users as consumers may feel that ads that suit their needs will be considered attractive and appropriate to their needs, but users may also see it as terrible and feel that the social media company has violated the privacy of its users (Tucker, 2014). With regard to user privacy, White argues that if users feel their privacy is compromised, users will reject the advertisement (Tucker, 2014). In this regard, the participants as social media users are also concerned about control over their lives in social media.

Conclusion

Research on user awareness and consciousness of personal information on social media shows that participants as social media users already know what personal information means according to their respective views. In addition, they are also able to provide explanations and examples of various personal data information. In interacting using social media, users often involve personal data information for various purposes. The involvement of this information is known to have a relationship at the stage of individual consciousness when interacting with social media. The stages of individual consciousness can be distinguished from the critical thinking stages that participants do in the activities of including personal information and data on their social media page. This stage underlies the reasons for the decision to include personal

data, which is based on the security factor of social media service providers and among their fellow users.

Concern for social media users is due to concerns over the potential misuse of personal information and data, which is closely related to individual privacy. They have also realized that sharing personal information and data on social media can trigger irresponsible parties to use this personal information. This concern also arises from the potential for social media service developers to use users' personal data for several purposes which could potentially harm their users.

Limitations

This qualitative study researchers wanted to see how the participants' views related to the issues of privacy and personal information as users of social media. This research on awareness of information was conducted with only a few participants so it could not describe or represent the overall condition of society.

Suggestion for Further Studies

In further research, a study or survey towards social media users can be carried out in order to get a broader picture of the awareness of personal information on social media users, especially in the case of Indonesia.

References

Altman, M., Wood, A., O'Brien, D. R., & Gasser, U. (2018). Practical approaches to big data privacy over time. *International Data Privacy Law*, 8(1), 29-51. doi:10.1093/idpl/ipx027

Beigi, Ghazaleh & Liu, Huan. (2018). Privacy in Social Media: Identification, Mitigation and Applications. *ACM Trans. Web 9*, 4, Article 39 (July 2018)

Bossetta, M. (2018). The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy. *Journal of international affairs*, 97-106.

Cavoukian, A. (2019, May 28). *Privacy and Digital Identity: Implications For The Internet*. Lake Maggiore, Italy.

Dhir, A., Torsheim, T., Pallesen, S., & Andreassen, C. S. (2017). Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults? *Front Psychology*. doi:10.3389/fpsyg.2017.00815

Dove, E. S. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *The Journal of Law, Medicine & Ethics, 46*, 1013-1030. doi:10.1177/1073110518822003

EU GDPR. (2018). *What is a data subject?* Retrieved Maret 2019, from European Union General Data Protection Regulation (EUGDPR): https://eugdprcompliant.com/what-is-data-subject/

Griffin, G. (2018, April 24). *Facebook is in Crisis Over Data Abuse Scandal and Harvesting of Information was Rife, Says Academic at Heart of It*. The Independent. Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-data-abuse-scandal-latest-cambridge-analytica-kogan-a8320066.html

Ho, G., Sharma, A., Javed, M., Paxson, V., & Wagner, D. (2017). Detecting Credential Spearphishing Attacks in Enterprise Settings. *26th USENIX Security Symposium* (pp. 469-485). Vancouver: USENIX.

ICO. (2018, Mei 24). *What is Personal Data?* London, England.

Janecek, V. (2018). Ownership of personal data in the internet of things. *Computer law & security review, 34*, 1039-1052.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology*, 109-125.

Kumar N, Senthil, Saravanakumar K, Deepa K. (2016). On privacy and security in social media – a comprehensive study, *Procedia Computer Science,* Volume 78, 114-119

Lupton, D., Pink, S., Labond, C. H., & Sumartojo, S. (2018). Personal data contexts, data sense, and self-tracking cycling. *International Journal of Communication, 12*, 647-665.

Milham, M. &. (2018). Managing the virtual boundaries: online social networks, disclosure and privacy behaviour. *New Media & Society*, 1476-1497.

Okditazeini, V., & Irwansyah. (2018). Ancaman privasi dan data mining di era digital: analisis meta-sintesis pada social networking sites (sns). *Jurnal Studi Komunikasi dan Media*, 109-122.

Pangrazio, L., & Selwyn, N. (2019). 'Personal data literacies': a critical literacies approach to enhancing understandings of personal digital data. *New Media & Society*, 21(2), 419-437. doi:10.1177/1461444818799523

Privacy International. (2018, Agustus). *Data Protection Guide.* Retrieved from Privacy International: https://privacyinternational.org/data-protection-guide

Sloan, L., & Quan-Haase, A. (2017). The SAGE handbook of social media research methods. Los Angeles: SAGE reference.

Tavani, H. T. (2013). *Ethics and technology: controversies, questions, and strategies for ethical computing* (4th ed.). New Hempshire, United States of America: Rivier University.

Tucker, C. E. (2014). Social Networks, Personalized Advertising, and Privacy Controls. *Journal of Marketing Research, 51*(5), 546-562. Retrieved from https://remote-lib.ui.ac.id:2094/stable/43832316

Quan-Haase, A., & Young, A. L. (2010). Uses and gratifications of social media: A comparison of Facebook and instant messaging. *Bulletin of Science, Technology & Society*, *30*(5), 350-361.

Van Aacke, Patrick & Trutens, Maarten. (2010). Privacy and social networks. *Computer Law & Security Review, 26*(5), 535-546.

Yeh, C.-H., Wang, Y.-S., Lin, S.-J., Tseng, T. H., Lin, H.-H., Shih, Y.-W., & Lai, Y. (2018). What drives internet users' willingness to provide personal information? *Online Information Review, 42*(6), 923-939. doi:10.1108/OIR-09-2016-0264