Jurnal Komunikasi Ikatan Sarjana Komunikasi Indonesia, Vol. 8 (1), 2023, 85-100

JURNAL
KOMUNIKASI
IKATAN SARJANA KOMUNIKASI INDONESIA

E-ISSN: 2503-0795
P-ISSN: 2548-8740

Digital Literacy Skills Against Children's Personal Data Protection on Social Media

http://dx.doi.org/10.25008/jkiski.v8i1.767

Likha Sari Anggreni[1,2*], Nunung Prajarto[1], Novi Kurnia[1]
[1]Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur, Yogyakarta 55281 - Indonesia
[2]Universitas Sebelas Maret Surakarta
Jl. Ir. Sutami No. 36 A, Kentingan, Surakarta 57126 - Indonesia
[*]Corresponding author: likhasari2020@mail.ugm.ac.id

Submitted: December 13, 2022, **Revised**: April 29, 2023, **Accepted**: June 13, 2023
Accredited by Kemristekdikti No. 28/E/KPT/2019

Abstract

The popularity of social media attracts many people to participate in various activities every day. Social media usually comes in the form of audio, graphics, video text and animations that provide convenience to its users to disseminate and access information quickly amd easily. Without realizing it, parents often show off their children's personal data in their parents' and children's accounts, usually for personal or business purposes. The purpose of this study is to examine more about the efforts made by parents to protect children's data privacy on Instagram social media accounts. This study uses the meta-analysis method of the literature study on previous studies. In this study, we want to see how the role of digital literacy in protecting children's personal data is and how to conceptualize children's self-protection digital literacy on social media. The findings of this study with the concept, threats, recommendations regarding the importance of digital literacy for personal data protection and conceptual integration can be used as a reference in further research. The protection of children's personal data is important to thwart the threat of cyber crime, violence and online extortion. It can also be one of the guarantees for children’s good growth and development because the data will not be misused by other parties for financial gain or to threaten children.

Keywords: Children’s personal data; Digital literacy; Personal data protection; Library study; Social media

Introduction

Social media is a medium for people to access information, produce messages and spread messages. Social media also allows users to create and share content by interacting with one another (de Vries et al., 2017; Peters et al., 2013). This information cycling has the drawback that it sometimes indicates that users are unable to find credible, useful information when it is needed. Social media platforms have become a necessity in everyday life so that people rely on them to meet every need, ranging from news, updates on events, such as entertainment, connecting with family and friends, reviewing product/service recommendations, new friendships, fulfilling emotional needs, to self-expression.

Social media platforms such as youtube, whatsapp, Instagram, twitter, and linkedin allow users to create content and are very influential in various settings such as user behavior, entrepreneurial activities, socio-cultural and political issues (Giunchiglia et al., 2018; Greenwood & Gopal, 2015). Uploads in the form of articles, user posts, photos, and videos can be recorded by social media platforms such as Facebook, Instagram, Twitter, and Snapchat. The total number of social media users is around 3,484 million. They spend an average of 2 hours 23 minutes per day accessing social media and sending messages and around 98% of them use 4 social media platforms every day (Werner Geyser, https://influencermarketinghub.com/social-media-statistics-2021/ accessed 20 June 2021).

Some of the messages exchanged on social media platforms are personal statuses, such as uploads seeking support, and people seeking help. The interesting thing is that these posts can be socially exhausting which creates excessive social burden and causes other users to experience negative behavioral and psychological consequences because they feel compelled to respond (Luqman et al., 2017; Maier et al., 2015).

Activities related to creating and sharing this content can occur in the process of interaction between users by providing comments to each other on their social media accounts. Self-expression on social media accounts is done by creating activities and contributing to activities. Users can express their own sense of freedom without any interference from external sources such as rules and instructions (Peters et al., 2013). What they convey is based on the experience and knowledge of each individual. Indeed, social media has a space in conveying information on the accounts of each of its users.

The ease of conveying this information is used by parents to share stories of family members, tell about their daily lives and share photos with other social media users. Not to mention that children who have social media accounts will also behave in the same way to share information with each other (Madden et al., 2012). Hence, in this interaction process it is possible to share personal information intentionally and unintentionally that will threaten the safety of the children.

This has given rise to policy discussions about how governments should act in the context of personal information about children and adults, which is widely collected, analyzed and shared in the cyclical digital economy. People's lives in America can be found using a simple search query by looking at traits and interests that are easy to find through social media posts and through the social networks they build. Unless they take special measures to prevent certain information from being tracked, internet service providers track most online behavior and collect information for specific purposes.

The collection of information in the United States about children under the age of 13 is subject to regulations under the Children's Online Provacy Protection the Act that has been in effect since 2000. The Act requires service providers to obtain parental consent before obtaining information about children under the age of 13 years. Some social media platforms, such as Facebook, Instagram and Twitter require users to be at least 13 years to use their sites, yet many minors continue to use social media and lie about their age, even parents deliberately create social media accounts for their children (Anderson & Jiang, 2018a). The Pew Research Center conducts studies on children, youths and parents regarding issues related to privacy, identity and information sharing, through digital media.

While in Indonesia, according to data from the Communication and Informatics Ministry (Kominfo), women have a higher level of vigilance than men in sharing personal data, but women are sometimes less aware of the dangers that lurk as a result of spreading personal data. Harassment in cyberspace, threats of violence, child trafficking, cyberbullying and digital kidnapping can stalk women and children in cyberspace if personal data is spread.

Personal data-related violations such as misuse of data, data leakage, act of buying and selling data can occur due to system errors, lack of system security, human negligence, intention, and low awareness of personal data security. Indonesia is drafting a personal data protection law to lay a strong basis for the protection of personal data and the prosecution of personal data violations (Kurnia et al., 2021). Several things that need attention to protect personal data are awareness; vigilance; understanding and knowledge.

This study will elaborate on how digital literacy is to protect children's personal data on Instagram social media. By first explaining the concept of digital literacy and protecting children's personal data which then spreads through social media, the conceptual explanation is provided. Based on the background, this study is limited by the following problems: What is the role of digital literacy in protecting children's personal data? How is the concept of digital literacy for child self-protection on Instagram social media?

Theoretical Framework

Children are starting to have an online presence at increasingly younger ages. Their online activities are not only about playing, creating, expressing themselves, experimenting with identities and relationships, learning, and revealing their personal data (Macenaite & Kosta, 2017). This situation is also seen in personal photo data, accompanied by names and history or family, developments from year to year that are likely uploaded by certain organizations that can actually be consumed by the public via the internet (Chege, 2018). Children's personal data becomes more vulnerable to being easily spread on social media. Data that should be the privacy of the child but has been freely published by his parents or by minors. Parents' literacy regarding personal data for children is also still minimal.

The threat of evil that is likely to be experienced by children is in sight. They may be less able to evaluate dangerous situations and are easy to mislead because they still lack awareness that their virtual actions will have long-term effects (Macenaite & Kosta, 2017). In the digital era, children's privacy is increasingly threatened by forms of collection, as well as data surveillance managed by parents and the state (including education, health, welfare, and legal systems) (Stoilova et al., 2021). For example, when making data on social media, data can be designed, tracked, collected and analyzed. The data can then give rise to new forms of economic value so as to create new market players to process data and some new consequences that arise. Even indifference arises by unscrupulous organizations that are less caring, less sensitive, less professional with the exploitation of using children's personal data for the benefit of their organization (Chege, 2018).

Milkaite explained that the child's personal data has now become a data bank that is collected and processed in unprecedented numbers so that it becomes a phenomenon called datafication and quantification of children's daily lives from a very early age (Milkaite & Lievens, 2018). The issue arises with the increasing adoption of digital devices that embrace applications and platforms for various purposes and are most likely to use, analyze, and infer information about users. However, the profile of the child data that has been collected is a concern because it can be used for various purposes such as behavior that is so sophisticated that it can influence people's choices and especially children's choices without them realizing it. Building a profile of a child's personal data from a very young and growing age can lead to potentially discriminatory practices in the future. Smyr added that the increasing threat to children's information privacy protection in the gaming industry is gradually expanding its borders with the industry's existing problems.

Personal data is a privacy, that is, a protective right. Privacy should be maintained and protected by each person. However, there is a shift accompanied by increasing concerns about people's control over personal information and privacy violations that occur as a result of oneself, others both individually and organizationally intentionally or unintentionally (Stoilova et al., 2021). So it is important to use technology safely and responsibly to maintain online privacy. Children need to learn about data and online privacy to protect their rights. The situation can be overcome with parental assistance and enforced regulations.

Digital Literacy Skills

The ability to understand digital literacy is quite important when surfing using new media. Especially when dealing with social media and conveying things that are sensitive enough to upload. Understanding how to cultivate literacy skills is a shared awareness. Literacy skills are not only needed by children, parents, people around the environment as well as organizations and government. Technology not only makes us smarter but also how to be wiser in how to use it or how to deal with similar situations (Tzifopoulos, 2020).

According to a study conducted by Tzifop Oulos, a male gender teacher with an additional degree, has a high self-confidence without fear of technology by adopting the view that technology is necessary in modern practice. Although the level of literacy towards technology is high, not being able to use it will hamper the teaching process.

Digital literacy skills serve as basic literacy equivalent to reading, writing and arithmetic. The adoption of digital literacy skills used to improve quality is an important issue for the digital learning environment (Techataweewan & Prasertsin, 2018). Digital literacy is also often seen as a minimum skill that allows users to operate more effectively in the use of software as well as how to perform various basic information retrieval tasks. This issue has several critical elements such as critical thinking skills, creativity, building and evaluating information, and using digital media effectively (Lim et al., 2022).

There are several components of digital literacy skills mentioned by Alkali including: (1) visual photo skills (reading graphic displays); (2) reproductive skills (utilizing digital devices to make new and meaningful findings from pre-existing ones); (3) branching skills (building knowledge from non-linear, hypertextual, and navigational); (4) information skills (evaluating the quality and validity of information); (5) social-emotional skills (understanding the rules that apply in cyberspace and applying this understanding in online cyber communication) (Eshet-alkali & Amichai-hamburger, 2004).

Material and Methodology

This study uses a library study, which analyzes research that has been done previously, or previous research related to children's personal data and Instagram social media. The data obtained are secondary data, namely from the previous research. The concept of meta-analysis used in this study is a secondary integrative analysis. The aim is to answer research questions with pre-existing data. The study of children's personal data on Instagram social media was carried out by analyzing the data on the findings of the studies that had been carried out.

Meta-analytical methods are useful in combining evidence to inform social policy. In this method, it is necessary to pay attention to scoping and targeting appropriate research questions in the meta-analysis, choosing eligibility criteria where the main study varies in research design and choice of finding size and identifying sources of heterogeneity in the findings of previous studies (Davis, Mengersen, Bennett, & Mazerolle, 2014).

Findings from previous studies can be used as a basis for supporting or rejecting the hypothesis in the study.

The steps of conducting meta-analysis are: (1) Determination of research questions: What are the problems that discuss the protection of children's personal data in the existing research? How is the concept of digital literacy on the security of children's data privacy on social media?; (2) Carry out a literature search, using Google Schoolar and keyword data on child privacy, social media and digital literacy. The choice to use Google Scholar is because the site allows results with a variety of journals, not limited by certain publishers. So the author does not need to look at the site of each publisher to find articles; (3) Screen articles by explaining the concept of protecting children's personal data, digital literacy and Instagram social media. The selection of the article is focused on discussing digital literacy on social media, then focusing on discussing children's data privacy on social media; (4) Do a synthesis by looking at the abstraction of the article, then review and compile the results. After synthesizing based on these criteria, it produces as many as 10 primary study articles that match the criteria.

Table 1. Discussion Focus of Privacy Data

Author	**Publication year**	**Discussion focus**
Suciati	2019	Privacy data
Salleh, Abdullah, Salman, Hasan	2017	Awareness and Knowledge of Privacy Through Social Media
Ilham and Salleh	2017	Privacy and security of app users on social media
Irwansyah	2020	Privacy data
Yang, Bingqing Qu	2015	Public and private data activity on social media
Zhang,	2018	Disclosure of data on social media, is a threat to user privacy
Sofian, Pratama	2020	Online privacy data protection

Jong-Youn Rha	2020	Online privacy of children's users
Jason Nolan	2011	Children's autonomy in using online media
Keith	2017	Child self-protection by parents on social media

Source: Journal (processed by researcher)

Result and Discussion

Conceptual Digital Literacy

Communication technology is growing rapidly along with the development of digital technology, which presents new ways of communication and new media that are no longer limited by time and distance. The emergence of social media as a medium of expressing opinions gives freedom to its users. However, this freedom requires limitations and ethics that are applied when using social media. A lot of information is present in everyday life, with a variety of information that is sometimes excessive to the individual, even information that does not need to be conveyed. So at times like this, the individual's ability to choose information is a challenge in itself (Liu et al., 2017; Schmitt et al., 2018).

Information overload enters the era of communication abundance, which is characterized by communication that exceeds the threshold. Communication reaches a saturation point in society and its mind. This situation is caused by the continuous explosion of communication brought by the media into contemporary human life space, so that experts call this communication and society a media saturated society/media saturated environment/media filled society. The latest society is a society that is overflowed with a lot of information in the form of images, texts, sounds, signs, and visual messages and is flooded with information with ideological, political and commercial messages (Wijaya, 2019).

Currently, the Internet is a new medium that has become a necessity for most people around the world. Data from hootsuite in January 2021 shows that 59.5% of the total world population uses the internet. Meanwhile, 73.7% of the total Indonesian population is internet users (Social & Hootsuite, 2021). Apart from the large number of internet users, the challenge is that there is a need for understanding and actions from users because technology is a tool that does not determine how internet users will act. Therefore, a series of understandings and actions are needed by applying various media literacy, especially digital one. The importance of digital literacy is not only to see how much its users are exposed to digital media but also through literacy they are expected not only to be critical when using the information they access ,but also to not merely believe in one source of information with one perspective (Wijaya, 2019).

The concept of digital literacy is now very commonly used, introduced by Gilster in 1997. However, a number of authors have used the term digital literacy, this concept means the ability to read and understand information in hypertext or multimedia formats that are then available. Digital literacy is about mastering ideas, not pressing keys, so distinguishing its conception from a more limited view of technical skills from digital literacy is still the basis for most information literacy approaches to date, despite much elaboration, extension, and refinement, and to varying degrees. Different variants in detail and emphasis are usually involved, adding extra aspects e.g. divide "finding information" into "selecting resources" and "searching" and "accessing identified items" or adding aspects such as "communicating information" or "saving/archiving/deleting information", where they are important in certain contexts. An example is the “seven pillars” model, developed by Sconul (college, national and university library) in the UK, which distinguishes the following seven aspects: recognizing information needs; distinguishing ways of addressing gaps; developing a strategy to find; access; compare and evaluate; organize, implement, and communicate; synthesize and create.

Media literacy is not only the simple development of interpretive skills but also involves digital production skills such as the ability to create, be critical and contribute and consume digital content (Suwana & Lily, 2017). Digital literacy is also a basic/traditional skill developed in socio-cultural networks that emerged from traditional literacy such as reading and writing, skills in research and in critical analysis of media (Nolan et al., 2011).

These internet users are required to have skills in using the internet and digital media in carrying out digital media mediation processes that are carried out productively (Adikara et al., 2021). Users who have good digital literacy are able to use not only technology/tools but also digital media in a responsible way. To determine user's skills in digital media, there are four major maps of digital literacy competencies. According to Japelidi, the Network of Digital Literacy Activists (2018) states that there are 10 competencies, namely accessing, selecting, understanding, analyzing, verifying, evaluating, distributing, producing, participating and collaborating. Then Tular Nalar (2020) in Kusumastuti (2021) states that there are eight competencies, namely accessing, managing information, designing messages, processing information, sharing messages, building self-resilience, data protection, and collaboration (Kurnia et al., 2021). Furthermore, the National Cyber and Crypto Agency (BSSN) (2020) in Aksara (2021) states that there are five competencies, namely managing information data; communication and collaboration; content creation; digital security; and participation & action. Finally, Kominfo, Siberkreasi & Deloitte (2021) stated that there are four areas of competence, namely digital skills, digital culture, digital ethics, and digital safety (Monggilo et al., 2021).

Digital skills indicator areas are a basic knowledge of the digital landscape, the internet and cyberspace; a basic knowledge of information search engines, how to use and sort data; regarding conversational applications and social media; a basic knowledge of digital wallet applications, marketplaces and digital transactions. Digital culture is a basic knowledge of Pancasila values and Bhinneka Tunggal Ika as the basis for digital skills in cultural, national and state life; digitalization of culture through the use of ICT; basic knowledge that encourages behavior to love domestic products and other productive activities as well as digital rights. Digital ethics is internet ethics; A knowledge of information containing hoaxes, hate speech, pornography, bullying and other negative content; interact, participate and collaborate in the digital space in accordance with the rules of digital ethics and applicable regulations. Meanwhile, digital safety is a basic knowledge of hardware protection features; a basic knowledge of digital identity protection, and personal data on digital platforms; a basic knowledge of digital fraud; a basic knowledge of digital track record in media (downloading and uploading).

Audiences need a well-developed configuration of communication and problem-solving skills based on the aforementioned digital literacy competencies. Digital literacy programs also need to go through a process of socialization and information and communication technique skills regarding how to use technology and including the context in which and when to apply skills, knowledge and information. As such, these digital media users have the confidence to operate safely in their digital environment.

Social Media

Social media is a new space for communication (Carr & Hayes, 2015) states that social media is an internet-based mass-personal communication channel, untrained and persistent on the perception of interaction between users and derives value, especially from content uploaded by users. It allows users to interact opportunistically and present themselves selectively in real-time or asynchronously with wide and narrow audiences.

Social media can play an important role in changing one's lifestyle, because of the ease with which it is easy to connect with one another. Social media refers to the ease, efficiency, electronic tools that can broadly facilitate anyone to publish, access information, collaborate on joint business or build relationships (Siddiqui & Singh, 2016).

The social media landscape is characterized by rapid change, as existing social media platforms are expanded with new interactive functions or replaced by new platforms. Social media platforms have the characteristics of facilitating social interaction, sharing ideas, forming and maintaining relationship/interest groups, developing one's presence, reputation and identity (Kietzmann et al., 2011). Social media has had a profound influence on the way we communicate, helping to break down the geographical barriers that once limited communication and have led to an explosion of electronic participation, virtual presence, and online communities (Alalwan et al., 2017; Dwivedi et al., 2015). This changing transformation of communication by social media makes people browse and contribute to their social media accounts regularly, even some people prefer to communicate through social media rather than participate in face-to-face interactions. Social media communication is considered more challenging because emotions can be difficult to understand and detect (Dwivedi et al., 2018; Kapoor et al., 2018).

Social media can make a person feel less lonely or alone and create a space to interact with people and allow people to connect with friends easily and make new friends (Anderson & Jiang, 2018b) mentions the most popular social media accounts among people, teenagers namely Youtube, Instagram and Snapchat. 95% of teens access social media using smartphones and 45% say they are almost always online throughout the day. Facebook is no longer the dominant online platform among teenagers as shown by the Center's Survey 2015 and 2018 that teenagers access Facebook only about 20%.

According to data on we are social #Digital2021 January 2021, the number of active Instagram users are 170 million, accounting for 61% of the total Indonesian population. The highest number of users are at the age of 18-34 years, reaching 64.8% of the total. The most viewed platforms are Youtube (93%), Whatsapp (87%) and Instagram (86%). Meanwhile, Facebook is in fourth place with 85% (Social & Hootsuite, 2021).

Protection of Children's Personal Data

Personal data is the human rights of every human being to be protected and requires the willingness of the owner to share it with others. The data in question is in the form of identity, codes, symbols, letters and numbers that are personal markers of someone that are personal. Indonesia is still in the process of drafting a personal data protection law, in an effort to regulate personal data protection.

There are different international and national regulations regarding the privacy of personal data. In Europe, the General Data Protection Regulation (GDPR) seeks to protect personal data and works against unauthorized disclosure, identity theft and online abuse (Ferrari et al., 2013) (European Union 2016, 2018). The GDPR applies to children and stipulates that they need consent from a legal guardian to use online services until they are 16 years of age or younger in certain countries. In the United States, the Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA) are the main regulations governing the protection of children's data.

Indonesia already has personal data protection rules in the digital era in the form of Ministerial Regulation *(Permen)* No. 20 of 2016 concerning Personal Data Protection (PDP). The regulation began to take effect on November 7, 2016. Personal data is certain individual data that is stored, maintained, and kept true. and kept confidential. The owner of personal data is an individual with certain personal data attached. According to the Ministry of Communication and Information, every electronic system operator must have internal rules for the protection of personal data in implementing the system. These rules are a form of prevention to avoid failures in the protection of personal data. Data mining by the operator of the electronic system must comply with the provisions of the legislation. This rule stipulates that an electronic system that can be used for the protection of personal data is the system that has been certified, and has internal rules that must pay attention to the aspects of human resources, application of technology, methods and costs. On the other hand, the owner of personal data has the right to confidentiality, the right to file a complaint in resolving personal data disputes and gain historical access, as well as the right to the destruction of his/her data. Parents/guardians are the givers of consent for children's personal data. FERPA and COPPA have been in place before the advent of many technologies such as smartphones, social media and other applications.

Digital identity is divided into visible identity and invisible identity. Visible identities are account names, user profile photos, user descriptions, other identities listed in the account, while invisible identities include PIN/password, two factor authentication, OTP and other identities.

Personal data is data or certain individual information that is stored, maintained, and protected in confidentiality because it is private and unique. The form of personal data is divided into general personal data and special personal data. General personal data is in the form of name, gender, nationality, religion, date of birth, occupation, home address, email, telephone number and others. While specific personal data is in the form of health data, genetic biometrics, finance, race/ethnicity, sexual preferences, political views, family data, crime data and others.

The ease with which information can be accessed and distributed on social media is not spared by the children who use these facilities. Although social media should have a user age provision, in practice many children under a predetermined age already have their own account, whether it is managed by themselves or their parents. The group of such children are vulnerable to digital crime due to inability and ignorance in using social media. As a result, they are not aware of the dangers threatening their safety when using digital media. Among them are bullying, child trafficking, theft of personal data. First, bullying is defined as an unpleasant behavior, both verbally and physically, that is received by someone. Bullying cases on digital media are caused by uploading personal content which is then distributed and various kinds of comments appear, causing bullying.

Discussion

Suciati (2019) states that the convenience and facilities provided by the internet accompanied by acts of self-disclosure on social media such as sharing personal information, posting events and activities that they do can pose a risk to their privacy. The act of intentionally sharing personal information with others is a self-disclosure associated with privacy risks on social media.

Privacy issues on social media: (1) Individuals upload information about themselves, The information is found, thus causing them trouble and to get into trouble. Risk: Sexual predators and cyberbullying (Bazarova, 2016; Ebrahimi, 2018). According to the National Society for the Prevention of Cruelty to Children (NSPCC), the Internet has become a popular social media for child predators to find their sexual victims; (2) The practice of uploading content about other people on one's social media accounts. on Instagram, facebook, flickr platform allows users to associate other accounts/usernames in uploaded photos, images or videos with the tag feature on social media platforms. Risk: without consent, threatens privacy as it allows wide exposure of aspects of private life that were previously closed; (3) The emergence of user's suspicion of social media platform services that they feel investigated and the use of their personal data. Risk/case: MySpace developed a method of data mining user profiles for demographic information that advertisers can exploit.

Privacy conceptualization: (1) Rights related to security, safety, personal space, and personal information (Fulton & Kibby, 2017). The boomer generation interprets privacy as confidentiality, private confidentiality from the public, but the millennial generation sees this privacy as a commodity, which can be exchanged for online friends for social capital which can then be utilized for organizational and business purposes; (2) Personal problems and freedoms are not undermined; (3) A culture-specific phenomenon, when social media becomes a global and popular necessity, the practice of privacy is in an important cross-cultural context.

Internet services such as services convert personal information into business needs from the social media platform itself. Selling advertising space with information from user profiles and entries from the platform. Keywords used, location, interests, gender, relationship status, activity, employment information, other demographics.

The presence of someone on social media is highly anticipated by data suppliers, because it can be utilized where data is commodified through the redistribution of power in the information age. Data on behavior and daily life can be monitored, when and where to access the internet, shop online, buy food online.

Hasan (2017) Security and privacy risks have an impact on users because information and activities can be accessed by others through social networks easily. There is a drive of bad intentions to steal identity, access data and misuse information. Social media provides a wide space for other individuals/ third parties to read, share, and save data. Information is disseminated because of hobbies and interests to establish deeper relationships. Information shared is related to school, personal information.

The awareness are (1) Become a major issue/ concern for the future; (2) Third person can access personal information on social media; (3) The appearance of advertisements and promotions (pop-ups/ spam) can threaten privacy; (4) The need to control privacy settings when using social media/ internet; (5) Have the skills to control personal information when using the internet; (6) Have a knowledge of the privacy issues of personal information to deal with the digital environment.

The solution given by Hasan, when he has information literacy skills and media literacy can filter information to be shared on social media. Awareness will exist if you understand the importance of the privacy and security aspects of personal information. In the past, surveillance was on CCTV, but now the camera is in the hands of all smartphone owners around the world.

Ilham mentions (Madiha et al., 2015) the informant's experience as a social media user about how are the events around them. There are (1) Stealing pictures on social media and using pictures as profile pictures; (2) Data stored on computers or smartphones that should be personal information can become public consumption.

The second thing is about the informant's perception of the issue of privacy and information security (1) The negative things that happen on social media include feeling worried about the leakage of bank account information and phone numbers when making transactions and buying and selling goods on social media; (2) Personal data and security Return to each user, so that they are maintained and are not misused; (3) Policies that play a role in controlling the issue of protecting the privacy and security of social media users

Three suggestions/recommendations from informants: (1) Self-control is the best mechanism of limiting the risk of data privacy and information security on social media; (2) Control of content on social media, that users must be wise to control the content they upload.

The implication of the study is first, the impact on the interests of media literacy from children to adults. Second, education should integrate the interests of media literacy, and ethics when using the positive and negative impacts of social media

Irwansyah mentioned that there was a data privacy violation at the time (Winarsih & Irwansyah, 2020): (1) Combined with external data that gets new conclusions about users (which should be confidential, and should not become public consumption); (2) Used to add value to a particular business; (3) Sensitive data is stored and processed in less secure locations so that the possibility of leakage is still high

It is almost impossible to carry out daily activities without disclosing personal information (so it is voluntary). Privacy relates to consent, people have the right to consent to provide the requested personal data. There is a tendency for people to be lazy to read the rules given by the platform because they are too long. Privacy model: surveillance (focus on tension between observer and supervised, public and private space), capture (modification of activities, purpose of data collection is not clear), datafication (focus on creating new anonymous personal information, reinterpretation and statistical analysis of data and its nature commodified personal information) have complementary meanings because different models help to understand and appreciate the notion of privacy, each model has a different point of view and focuses on specific features of socio-technological phenomena.

Privacy in data creation is divided into two: (1) Active, data owner is willing to provide data to third parties; (2) Passive, a situation where the data is generated by the online activities of the data owner, for example: browsing data but the data owner is not aware of the data being collected by a third party.

How to protect: firstly access restrictions; secondly, using anti-malware and anti-virus software. There are security tools that data owners can use to falsify their data: (1) Socketpuppet tool, hides the online identity of individuals by fraud. An individual's online activities are actually kept secret by creating fake identities and pretending to be someone else. By using this tool, data owned by one particular individual is considered belonging to a different individual. This will result in data collectors that have no knowledge to associate different sockets with one person. Thus, the actual activity of the data owner cannot be found in an easy way; (2) Maskme, allows users to alias their personal information such as email addresses or phone numbers. The data owner can use this mask whenever information is needed. This will be useful if the data owner needs to provide details of debit/credit card when making transactions online.

Data protection in modern information systems, data centers play an important role in retrieving a large amount of data. Privacy protection in the data processing section is divided into two phases, the first is to protect information from unsolicited disclosure because the data collected may contain sensitive information about the data owner.

Both aim to extract meaningful information from data without violating privacy.

Zhang mentioned that full disclosure of social media data can exacerbate threats to user privacy (Zhang et al., 2018). Some complete social media data is available and explicitly disclosed such as age, location, language, political preferences.

Privacy protection measures: (1) By using anonymous user IDs, the aim is to prevent crime/bad guys from linking anonymous IDs to appropriate users on real social networks; (2) Through his research is an effort to protect the privacy of text information.

Yang, Bingqing Qu explained in his article on user activity with public data, there is a perception that social media profiles are personal, such as gender, income level, political views and social contacts (Yang et al., 2019).

There is an inherent correlation between public and private data which often causes data leakage. (1) One's political affiliation can be deduced TV rating shows; (2) A person's gender can be inferred from activity on location-based social networks; (3) Personal data is often subject to inference attacks, where the enemy analyzes the user's public data to gain an unauthorized knowledge of his personal data.

Provides protection of personal data by distorting published data at the expense of the loss of utility of public data in the final processing stage. Challenges in maintaining data privacy: (1) Users still have different privacy issues, certain types of data such as gender are considered private by some users, other users prefer to consider it as public to get better service. So it is necessary to provide customizable privacy protection that is to protect personal data specified by the user only; (2) When subscribing to third party services, users often allow the service provider to access not only their historical public data but also their future public data as data streams.

Child Data Protection

Sofian (2020) explained in his article regarding the protection of children's personal data online that information that is attached to the child, is in the form of names, addresses, photos, videos and other information including thoughts that are written online such as text, sound and so on (Sofian et al., 2020).

The threat will appear when a child's personal data is spread. First, there is the potential to become a victim of various forms of crime in cyberspace. Children's activities, habits and tendencies to do something are stored by third parties and can be misused. Second, based on UNICEF data in 2017 on losses from children's personal data crimes, there were 5 child accounts stolen later in the United States, Javelin Strategy 7 Research found that one million children fell victims of identity theft, with a total loss of up to US $ 2.6 billion, while in the same year Europe experienced data theft of up to 1.37 billion data.

The habit of using technology facilities such as smartphones, PCs and tablets that are connected to the internet and used by children makes personal data and children's privacy difficult to separate, coupled with the Covid-19 pandemic which requires schools to conduct distance learning using smartphone/PC devices and software such as youtube, whatsapp or other applications that support the learning process.

The protection of children's personal data has not been specifically regulated in the law, resulting in arbitrary practices in the use of children's personal data, especially in the use and misuse of children's personal data online through social media. First, privacy is important in children's psychosocial development to ensure that they have the freedom and autonomy to explore and try out various possibilities for themselves in search of identity without running the risk of supervision or exposure. Second, improve social communication skills with others through social media, develop and maintain relationships with their friends, freely choose how much information about themselves to share, with whom and under what circumstances. Last, privacy is important to core democratic values such as autonomy, self-determination and dignity.

The general elucidation of the child protection law explains that because children, spiritually, physically and socially have yet to have the ability to stand alone, it is the obligation of the family, community and state to guarantee, maintain and secure the children. The personal data protection bill is in the process of being deliberated at the House of Representatives (DPR). Personal data protection is described as another form of privacy protection. To protect children's personal data, it is important to explain the concepts in regulations and policies. Several

European Union countries, the United States and the United Kingdom have regulated the protection of personal data, including children's personal data.

According to the General Data Protection Regulation (GDPR) in Europe, article 6 stipulates that data processing must be based on the legitimate interest of the data subject or owner of personal data. Other provisions in the United States through the Children's Online Privacy Protection Rule (COPPA) 2019 rules, explain the definition, notice and parental consent requirements, and Limitations of liability in the safe harbor doctrine (with actual knowledge of the operator). According to COPPA, the provisions that are protected in the protection of children's personal data are email address, first name, last name, layer name, location, message details, residential address, telephone number, hobbies, photos, videos, and audio. Meanwhile, according to the Information Commissioner's Office, UK, the protection of children's personal data includes: children's interests, transparency in data use, minimum data usage, data sharing, location, parental supervision, behavioral engineering techniques so that children act as they wish and online-connected toys.

The personal data protection in Indonesia is set forth in Article 2 paragraph (2) of the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems: Since the personal data of each child has been recorded in the database of the site or application operator, the government, parents or guardians must provide protection of personal data based on the principles of protection: (a) Respect for personal data as privacy; (b) Personal Data is confidential according to approval and/or based on; (c) provisions of laws and regulations; (d) Based on approval; (e) Relevance to the purpose of obtaining, collecting, processing; (f) Analysis, storage, display, announcement, delivery, and dissemination; (g) Eligibility of the electronic system used; (h) Good faith to immediately notify the owner of personal data in writing for any failure of personal data protection; (i) Availability of internal rules for the management of personal data protection; (j) Responsibility for personal data that is in the control of the user; (k) Easy access and correction of personal data by the owner of personal data; and (l) Integrity, accuracy, and validity and up-to-date of personal data.

Jong-Youn Rha (Rha et al., 2020) then tries to classify and analyze issues related to children's online privacy issues in Korea through case studies of applications used by children. First, child identification problems. Second, notification and approval effectiveness and the last Children's rights as information subjects

Under the United Nations Convention on the Rights of the Child, children have the right to be protected by taking into account the best interests of every member of society, even in various situations when using online services. In the United States, the Children's Online Privacy Protection Act (COPPA) has been in effect since 1998. In the UK, there are institutional measures that guarantee children's rights to be protected in the context of personal information so as to form a social foundation for children to grow up as mature members of society. in the future. Meanwhile, in Korea, efforts to protect children in the online environment are stipulated in the Information and Communication Network Act and the Location Information Act. Children are concerned with their limited abilities that they do not clearly recognize the risks and consequences of processing personal information and user rights.

In Korea, children are not sufficiently guaranteed of their rights to be protected. Although children's online activities are increasing, there is a lack of discussion about institutional and practical measures to protect children in the online environment. Protection of children's privacy rights includes user rights such as consent, withdrawal, viewing and error correction regarding the collection and use of children's personal information. Protection mechanisms, according to child identification, have limitations. The online child protection mechanism consists of procedures for securing a seal of approval from legal guardians and imposing restrictions on use of personal information after the child is identified.

The results of the case study show that the applications used by children are checked separately after downloading the applications. First, there is no guardian or parental consent and no age verification. Second, effective notification and consent procedures for the collection and use of personal information are required. Because the current privacy policy notice contains a lot of content in an ineffective way, users often agree formally without knowing the content, and the use of non-login methods, social login.

Third, it is necessary to consider the rights and interests of children. Children's data must be considered especially from a long-term perspective. That way children's personal information is not filtered or used as it is by storing and collecting children's personal information in services used during childhood because children are incomplete creatures in the growth process. Education about the importance of procedures for membership withdrawal and Personal information retention institutions for children and parents should be provided adequately to raise awareness of the importance to protect personal information.

Jason in his study explains that dependence on a supervision-based approach to monitor children's online activities (5-14 years) can cause greater harm, that is lost opportunities for children to have experiences that greatly help them in developing autonomy and independence. In this study, we want to see the social implications of limiting, supervising and controlling children's inline activities versus maintaining individual autonomy through parental assistance and critical reflective software and the use of social technology (Nolan et al., 2011).

The increasing presence of children in online and virtual environments raises questions about the types of content or activities that children should access and ideas about preserving innocence. The child's desire to metamorphose and re-label the spaces, practices and materials of everyday encounters as a critical dimension of childhood needs to be part of adults' awareness of children and should inform all of their interactions. Regardless of the context, it is children's interactions with the world that shape the extent to which children become the kind of social actors they expect to be in a particular social environment or cultural context.

In a study by Jenkins (2010) in Nolan, he noted the relationship between learning and autonomy to harmful perceptions that limit children's learning experience (Nolan et al., 2011). Autonomy is critically linked to child development in a number of areas: identity formation, independence and responsibility, individuation, and resilience & self-expression. Gaining autonomy especially the joint development of relationships between children and families, children and communities, and children's and socio-cultural contexts provides opportunities for children to have the most dynamic and meaningful involvement. All children need to engage in non-judgmental dialogue on issues that matter to them, in a language and way that they can understand and allow them to begin making ethical critiques and choices.

Children will show the need for privacy and autonomy in the early years through autonomous acts that are carried out and in response to heteronomy, namely as emancipatory actions or defiance of authority in the form of making chaos and noise, running away when called upon, and others. It becomes important whether it is possible to maintain authentic autonomy in a supervised space if there is no possibility for a child to engage in defiance through secrecy or subversion.

There is information implicit in obtaining information through supervision, not through voluntary disclosure, that children cannot be trusted to share with their parents. If parents really learn most about their children's activities directly from them than through supervision, then supervision can actually reduce what parents know about their children. This is because child self-disclosure requires and strengthens trust and respect between parents and children. Supervision that is hidden as an attitude of disrespect, distrust and patronizing can potentially contribute to a child's reluctance for open disclosure.

Children need to be trusted to understand trust and how to trust others. It involves experimentation, practice, testing, failure and reflection in contexts where some form of authenticity exists, with negotiated interpersonal guidance or mentoring with emotionally attached people. Guided and guided use of social media can be a supportive learning opportunity that leads to trust and autonomy rather than exercise in control and supervision. These alternatives to supervision can take many forms and there are a variety of strategies that parents can use.

Monitoring a child's activity online can be approached as a series of choices with established developmental and behavioral consequences. The strangest danger for children comes from adults, when they choose not to see children as individuals who must learn about the world around them through experimentation, testing and reflection and through exercising autonomy. Regardless of a child's cognitive capacity or level of socio-emotional development, it is the duty of adults to see and involve children as social actors and push them to the limits of their ability to see themselves online and offline.

But on the other hand Keith mentions that children often have a digital footprint long before they take the first step. Expert sources provide guidance for parents to understand social media, monitor children's use and provide advice to ensure children's social media use. However, there is a lack of resources in his study to help parents understand the potential consequences and healthy ways that parents can share information about their children. Disclosure that parents share online will follow their child into adulthood although there are benefits, there are also unconscious dangers, disadvantages that include identity theft, re-sharing of pirated information on predatory sites, sharing psychosocial information that should remain private and sharing revealing information. or embarrassing that may be abused by others (Keith & Steinberg, 2017).

The use of social media is common among parents, with children under 18 years of age. As many as 75% of parents use the internet through social media platforms, namely Facebook, Pinterest, LinkeIn, Instagram, and Twitter. From the use of new parents' social media in the context of social capital, it was found that 98% of mothers and 89% of fathers uploaded photos of their children to Facebook. Sharing photos and commenting on each other about children is one of the satisfactions in the role of parenting. However, when parents share information about their children online it is possible to disclose their children's personal information and often do so without their children's consent. Parents act as gatekeepers of their children's personal information and as narrators of their children's personal story. The dual role of parents in a child's online identity provides little protection for children as their online identity develops. A conflict of interest exists because the children of a finger may resent the disclosures made years earlier by their parents.

Some guidelines for parents and families are first to familiarize yourself with the privacy policy of the sharing site. Second, set up notifications to remind them when their children's name appears in search engines, can use google alerts. Third, parents who choose to share about their children's struggles should consider choosing to share anonymously. Fourth, be careful before sharing the actual location or full name of the children. Fifth, provide opportunities for children about the power of veto in online disclosure. Sixth, do not post pictures that show their children naked. Seventh, consider the various effects that can have an impact on self-esteem and well-being.

Conclusions

This article is expected to provide a contribution to further studies regarding the importance of digital literacy for the protection of personal data in new, more complex media. With an explanation of the concepts, threats, recommendations, regarding the importance of digital literacy for the protection of personal data and the conceptual combination in this study, it can be used as a reference for future research. The limitations of this study become an opportunity for further research, because it only describes how important digital literacy is to the protection of children's personal data in new media. Hence, in the future it can raise new media issues more specifically, as well as cases of violations due to the protection of children's personal data. The community needs to realize the importance of understanding the dangers and threats to children's personal data, so as to avoid any harm to children due to data exploitation through social media.

Protection of children's personal data is important to protect children from threats of cyber crime, violence, and online extortion. In addition, the protection of personal data can also guarantee the growth and development of children because the data is not misused by other parties for financial gain or to threaten children.

Realizing the importance of policies in the protection of personal data, such as in the developed countries of the European Union, the United States and the United Kingdom, which already have laws relating to the protection of children's personal data, it is also necessary for Indonesia to ratify a bill on child protection. As such, if other parties use the child's data, then they will be subject to sanctions.

The recommendations offered in this study are literacy, abilities and skills given to children regarding the importance of protecting personal data in order to avoid threats in the cyber world. This education is given not only to children but also to their parents and guardians so that they can provide self-protection, think when sharing information related to personal data. It also requires a future study to guide parents, policy makers and experts through the conflicts that are created when parents decide to disclose personal information about their children.

The next recommendation, when children use social media, is first, limit personal information, which is not to be rash when conveying personal information, such as providing telephone numbers, home addresses, school names, surnames, and other information that can be used by others to commit crimes and second, limit the use of smartphones. Third, identify safety threats, and then filter messages before sharing them, think again before sharing messages, see the source and the truth first.

Acknowledgements

This work was supported by the Ph.D Program Fisipol UGM (Grant number 4755/J01.SP/KEU-13/VIII/2020).

References

Adikara, G. J., Kurnia, N., Adikara, G. J., Kurnia, N., Adhrianti, L., Astuty, S., Wijayanto, X. A., Desiana, F., & Astuti, S. I. (2021). *Aman bermedia digital*. Direktorat Jenderal Aplikasi Informatika.

Alalwan, A. A., Rana, N. P., Dwivedi, Y. K., & Algharabat, R. (2017). Social media in marketing: A review and analysis of the existing literature. *Telematics and Informatics*, *34*(7), 1177–1190. https://doi.org/10.1016/j.tele.2017.05.008

Anderson, M., & Jiang, J. (2018a). Teen's Social Media Habits and Experiences. *PEW Research Center*, *November*, 33. https://www.pewinternet.org/2018/11/28/teens-social-media-habits-and-experiences/

Anderson, M., & Jiang, J. (2018b). Teens, social media & technology. *Pew Research Center [Internet & American Life Project]*, 1–9. http://publicservicesalliance.org/wp-content/uploads/2018/06/Teens-Social-Media-Technology-2018-PEW.pdf

Bazarova, N. N. (2016). Sharing Our Lives Online: Risks and Exposure in Social Media. *Journal of Broadcasting & Electronic Media*, *60*(1), 190–192. https://doi.org/10.1080/08838151.2015.1093490

Carr, C. T., & Hayes, R. A. (2015). Social Media: Defining, Developing, and Divining. *Atlantic Journal of Communication*, *23*(1), 46–65. https://doi.org/10.1080/15456870.2015.972282

Chege, N. (2018). Children's personal data: Discursive legitimation strategies of private residential care institutions on the Kenyan coast. *Social Sciences*, *7*(7), 1–19. https://doi.org/10.3390/socsci7070114

de Vries, L., Peluso, A. M., Romani, S., Leeflang, P. S. H., & Marcati, A. (2017). Explaining consumer brand-related activities on social media: An investigation of the different roles of self-expression and socializing motivations. *Computers in Human Behavior*, *75*, 272–282. https://doi.org/10.1016/j.chb.2017.05.016

Dwivedi, Y. K., Kapoor, K. K., & Chen, H. (2015). Social media marketing and advertising. *The Marketing Review*, *15*(3), 289–309. https://doi.org/10.1362/146934715x14441363377999

Dwivedi, Y. K., Kelly, G., Janssen, M., Rana, N. P., Slade, E. L., & Clement, M. (2018). Social media: The good, the bad, and the Ugly. *Information Systems Frontiers*, *20*, 419–423.

Ebrahimi, M. (2018). Sharing our lives online: risks and exposure in social media. *Information, Communication & Society*, *21*(12), 1747–1748. https://doi.org/10.1080/1369118x.2017.1405061

Eshet-alkali, Y., & Amichai-hamburger, Y. (2004). Experiments in Digital Literacy. *Cyber Psychology & Behavior*, *7*(4), 421–429.

Ferrari, A., Punie, Y., & Bre, B. N. (2013). *DIGCOMP : A Framework for Developing and Understanding Digital Competence in Europe* . https://doi.org/10.2788/52966

Fulton, J. M., & Kibby, M. D. (2017). Millennials and the normalization of surveillance on Facebook. *Continuum*, *31*(2), 189–199. https://doi.org/10.1080/10304312.2016.1265094

Giunchiglia, F., Zeni, M., Gobbi, E., Bignotti, E., & Bison, I. (2018). Mobile social media usage and academic performance. *Computers in Human Behavior*, *82*, 177–185. https://doi.org/10.1016/j.chb.2017.12.041

Greenwood, B. N., & Gopal, A. (2015). Tigerblood: Newspapers, blogs, and the founding of information technology firms. *Information Systems Research*, *26*(4), 812–828. https://doi.org/10.1287/isre.2015.0603

Hasan, A. (2017). Kesedaran dan Pengetahuan terhadap Keselamatan dan Privasi Melalui Media Sosial dalam Kalangan Belia (Awareness and knowledge of safety and privacy through social media among youth). *E-Bangi*, *14*(3).

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2018). Advances in Social Media Research: Past, Present and Future. *Information Systems Frontiers*, *20*(3), 531–558. https://doi.org/10.1007/s10796-017-9810-y

Keith, B. E., & Steinberg, S. (2017). Parental sharing on the internet child privacy in the age of social media and the pediatrician's role. *JAMA Pediatrics*, *171*(5), 413–414. https://doi.org/10.1001/jamapediatrics.2016.5059

Kietzmann, J. H., Hermkens, K., Mccarthy, I. P., & Silvestre, B. S. (2011). Social media ? Get serious ! Understanding the functional building blocks of social media. *Business Horizons*, *54*(3), 241–251. https://doi.org/10.1016/j.bushor.2011.01.005

Kurnia, N., Astuti, S. I., Monggilo, Z. M. Z., Prananingrum, E. N., Kusumastuti, F., & Adikara, G. J. (2021). *Seri Modul Literasi Digital Kominfo Japelidi Siberkreasi 2021-2024*.

Lim, Y. H., Lee, J. K., Ng, W., & Teo, T. W. (2022). Implementation of PCM in a Singapore school: Impact on students' learning outcomes. *Journal of Educational Research*, *115*(1), 25–36. https://doi.org/10.1080/00220671.2021.2019659

Liu, L., Liu, C., & Zhao, X. (2017). Mapping the paths from styles of anger experience and expression to obsessive-compulsive symptoms: The moderating roles of family cohesion and adaptability. *Frontiers in Psychology*, *8*(MAY), 1–10. https://doi.org/10.3389/fpsyg.2017.00671

Luqman, A., Cao, X., Ali, A., Masood, A., & Yu, L. (2017). Empirical investigation of Facebook discontinues usage intentions based on SOR paradigm. *Computers in Human Behavior*, *70*, 544–555. https://doi.org/10.1016/j.chb.2017.01.020

Macenaite, M., & Kosta, E. (2017). Consent for processing children's personal data in the EU: following in US footsteps? *Information and Communications Technology Law*, *26*(2), 146–197. https://doi.org/10.1080/13600834.2017.1321096

Madden, M., Cortesi, S., & Lenhart, A. (2012). Parents, Teens, and Online Privacy. *Interaction*, *9*(8), 29. http://www.crossingguardconsulting.com/wp-content/uploads/2013/01/PIP_ParentsTeensAndPrivacy.pdf

Madiha, N., Ilham, M., Azul, M., & Salleh, M. (2015). Isu Privasi dan Keselamatan dalam Kalangan Pengguna Aplikasi Media Sosial (Privacy and Security Issues among Users of Social Media Applications). *E-Bangi*, *12*(2), 203–216.

Maier, C., Laumer, S., Eckhardt, A., & Weitzel, T. (2015). Giving too much social support: Social overload on social networking sites. *European Journal of Information Systems*, *24*(5), 447–464. https://doi.org/10.1057/ejis.2014.3

Milkaite, I., & Lievens, E. (2018). Towards a better protection of children ' s personal data collected by connected toys and devices. *Digital Freedom Found*.

Monggilo, Z. M. Z., Kurnia, N., Wirawanda, Y., Desi, Y. P., Sukmawati, A. I., Anwar, C. R., Wenerda, I., & Astuti, S. I. (2021). *Cakap Bermedia Digital* (Z. M. Z. Monggilo & Novi Kurnia (eds.)). Direktorat Jenderal Aplikasi Informatika.

Nolan, J., Raynes-Goldie, K., & McBride, M. (2011). The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media. *Journal of Childhood Studies*, *36*(2), 24–32. https://doi.org/10.18357/jcs.v36i2.15089

Peters, K., Chen, Y., Kaplan, A. M., Ognibeni, B., & Pauwels, K. (2013). ScienceDirect Social Media Metrics — A Framework and Guidelines for Managing Social Media. *Journal of Interactive Marketing*, *27*(4), 281–298. https://doi.org/10.1016/j.intmar.2013.09.007

Rha, J., Cho, E., & Lee, S. (2020). Protecting Children's Online Privacy : Privacy Issues and Its Implications. *Journal of Digital Convergence*, *18*(10), 23–31. https://doi.org/10.14400/JDC.2020.18.10.023

Schmitt, J. B., Debbelt, C. A., & Schneider, F. M. (2018). Too much information? Predictors of information overload in the context of online news exposure. *Information Communication and Society*, *21*(8), 1151–1167. https://doi.org/10.1080/1369118X.2017.1305427

Siddiqui, S., & Singh, T. (2016). Social Media its Impact with Positive and Negative Aspects. *International Journal of Computer Applications Technology and Research*, *5*(2), 72–75.

Social, we are, & Hootsuite. (2021). *DIGITAL 2021 Global Overview Report*.

Sofian, A., Pratama, B. P., Besar, & Pratomo, F. C. P. (2020). Perlindungan Data Privasi Anak Online Dalam Mencegah Pelanggaran Hak Anak Children ' S Online Privacy Protection on Preventing Violation of Children Rights. *Media Informasi Kesejahteraan Sosial*, *44*(Perlindungan Data Privasi Anak Online dalam Mencegah Pelanggaran Hak Anak (Ahmad), 115–129. https://ejournal.kemsos.go.id/index.php/mediainformasi/article/view/2059

Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online–a systematic evidence mapping. *Information Communication and Society*, *24*(4), 557–575. https://doi.org/10.1080/1369118X.2019.1657164

Suciati, T. N. (2019). Sinisme Privasi, Diskriminasi Dan Komoditas Data: Paradoks Media Sosial Di Era Kapitalisme Pengawasan. *Journal Acta Diurna*, *15*(2), 145. https://doi.org/10.20884/1.actadiurna.2019.15.2.2138

Suwana, F., & Lily. (2017). Empowering Indonesian women through building digital media literacy. *Kasetsart Journal of Social Sciences*, *38*(3), 212–217. https://doi.org/10.1016/j.kjss.2016.10.004

Techataweewan, W., & Prasertsin, U. (2018). Development of digital literacy indicators for Thai undergraduate students using mixed method research. *Kasetsart Journal of Social Sciences*, *39*(2), 215–221. https://doi.org/10.1016/j.kjss.2017.07.001

Tzifopoulos, M. (2020). In the shadow of Coronavirus: Distance education and digital literacy skills in Greece. *International Journal of Social Science and Technology*, *5*(2), 1–14. https://www.researchgate.net/publication/341358736

Wijaya, S. H. B. (2019). *Seri Literasi Media: Dari Hoax hingga Hacking* (I. A. Satyawan (ed.); edisi pert). Buku Litera.

Winarsih, W., & Irwansyah, I. (2020). Proteksi Privasi Big Data Dalam Media Sosial. *Jurnal Audience*, *3*(1), 1–33. https://doi.org/10.33633/ja.v3i1.3722

Yang, D., Qu, B., & Cudré-Mauroux, P. (2019). Privacy-Preserving Social Media Data Publishing for Personalized Ranking-Based Recommendation. *IEEE Transactions on Knowledge and Data Engineering*, *31*(3), 507–520. https://doi.org/10.1109/TKDE.2018.2840974

Zhang, J., Sun, J., Zhang, R., Zhang, Y., & Hu, X. (2018). Privacy-Preserving Social Media Data Outsourcing. *Proceedings - IEEE INFOCOM*, *2018-April*, 1106–1114. https://doi.org/10.1109/INFOCOM.2018.8486242